

## **Kenya: A Rough Ride towards an Information Economy**

By Matunda Nyanchama, PhD

On January 17<sup>th</sup>, 2012 Kenyans woke up to news of desecration of a number of government websites. A hacker has taken liberty to expose the weaknesses in the security of government systems, reportedly after a short tutorial. The hacker, coming from Indonesia, later even thanked Kenyan technical news sources for effectively covering the story of the hack!

Soon the blogosphere was aflame with concerned, animated Kenyans and friends of Kenya as to how this would happen. They seemed even angrier considering the very basic nature of flaws that led to the security breaches. It is as if an untrained mechanic has been used to overhaul a car engine only for the engine to be fouled by the most amateur of mechanics.

This needs to be a wakeup call to all Kenyans, and especially those in leadership, to put in place solid processes, people and technology in defense of the motherland.

Kenya, the nation of M-PESA and other upcoming innovations, has taken major strides into the *information age*. Today, the country is perhaps one of the best wired on the African continent, what with a number of submarine cables that have docked on the Kenyan coast recently. These, in turn, have availed cheap bandwidth and high-speed access both into and outside the country. There is a growing tech-savvy young generation perhaps best epitomized by growth of use of social media such as facebook and twitter. Even the Kenya Defense Forces communications realizes the power of such media and has made it an outlet for updates of such things as the war in Somalia!

The government on the other hand has led an onslaught on Internet providers to avail bandwidth at affordable prices. This would lower entry barriers and allow for equitable access by *mwananchi* who would reap attendant benefits.

These benefits are many and varied, including electronic commerce (e.g. being able to transact on the Internet), and government and private sector service delivery among others. Properly harnessed, connectivity can spur productivity, enhance effectiveness and generate economic growth. It is noteworthy that the Ministry of Information and Communications has targeted a 10% contribution to the country's Gross National Product (GDP).

...

At the launch of the first sub-marine cable Kenya lit cyberspace with substantial malicious activity as noted by leading security product company Symantec. It was akin to shining light into the darkest corner in a house where nobody had cared to clean!

In many respects, lack of high speed Internet connectivity had left the country as a safe haven where we could deploy systems without worrying whether they were secured or not. System owners didn't have to incur added costs of security because of low risk of being hacked as the systems were largely out of reach for many a hacker on the Internet.

High speed Internet changed all this for, suddenly, a computer deployed in Nairobi can easily and quickly be reached by someone with high speed connectivity anywhere in the world. High speed Internet also means we can run more complex applications faster than we could do before such bandwidth came.

We need to realize that our commendable foray into the superhighway, presents its own risks that we appear not to be prepared for. These perils include the potential for unauthorized people to steal, alter or make unreachable information on computers that are not properly secured.

Stolen sensitive information can cause harm to the nation and or individuals. Further risks include embarrassment in the face of the world and loss of reputation. It will not be a coincidence if, with the spread of the story on the Internet, we hear more of the same in subsequent copycat acts.

More risks are associated with fixing any security violations and damage caused by hackers.

When systems are hacked, the extent of loss can be immense not simply to companies or governments but also to countries and its nationals.

...

With the end of the cold war, cyberspace has become the new frontier for combat. Thus, we hear of information warfare between perceived adversaries intended for various objectives, including espionage, embarrassing target enemies and a means of staying ahead of the opponent.

The new cyber frontier has made industrial espionage easier than it was before. Why travel to distant countries seeking information from rival companies when one can "hit" several countries from a single location, targeting intended victims with a lapse in cyber defences? All one needs is some expert knowledge, exploit code and a gap in security on target systems.

In national warfare, we can take a contemporary example from our country's foray into Somalia in search of Al Shabaab terrorists. The country is at war! And these would do anything to hurt the country and her people. They already bombed public places in Kenya, causing major damage, including taking lives.

Just imagine the Al Shabaab getting hold of information about our armed forces' movements and attack plans! Picture further were the group able to alter the information and what subsequent confusion would ensue to well-laid out plans! And suppose further that they able to jam information access to make it impossible to communicate!

There is more!

Imagine through cyber violations they were able to track (say) the path of key security and government personnel, even the country's leadership.

In the private sector, Kenyan banks have seen escalating losses lately. They suspect these are associated with increased use of technology. It is possible that some of these losses could be due to Internet-related security violations due hackers, be they in or outside Kenya.

...

All countries take seriously the risks associated with information protection. And they do so for many good reasons, including warding off information warfare and protecting the national economy.

On the economic front thinkers suggest that future economic competitiveness will be determined by how well countries use knowledge for advantage. Those that fully exploit knowledge, taking full advantage of the same, would have a competitive edge.

Knowledge is a creation from information which in turn is generated from data. It means that those that faithfully collect data, use methodical approaches to generate information and knowledge out of the data will stay ahead.

Therefore it is important that that information be accurate and authentic, that it be accessible to only those that need it and be available when required. Inaccurate data would generate false information and hence lead to misplaced decisions. Stolen information can give a competitor an edge.

Information protection remains a challenge to all countries, including developed ones. As one blogger mentioned, even some of the best protected systems like those of the US Department of Defence have been violated on more than one occasion. It is also conventional knowledge that most violations are never reported hence what we learn of may be a tip of the iceberg in cyber violations.

It is also true that no system can be 100% secure. An analogy is that of a house whose doors must be open to its residents for the house to be useful. Yet the same doors provide a vulnerability that could be exploited by burglars.

...



## Agano Consulting Inc.

1011 Upper Middle Road East, Suite 1124  
Oakville, Ontario, Canada L6H 5Z9  
Phone: +1-888-587-1150  
[info@aganoconsulting.com](mailto:info@aganoconsulting.com)  
[www.aganoconsulting.com](http://www.aganoconsulting.com)

## Agano Consulting Ltd

Limuru Road, Suraj Plaza, Suite T16  
P. O. Box 62423, Nairobi, Kenya  
Phone: +254-20-2502435  
[info@aganoconsulting.com](mailto:info@aganoconsulting.com)  
[www.aganoconsulting.com](http://www.aganoconsulting.com)

These facts should not deter action on information protection. The fact that others (and especially advanced countries) are also violated remains cold comfort for Kenya when it faces the embarrassment and potential negative impact from the desecrations of the kind reported in the press.

The practice of information protection has substantially matured. All the country and its private sector need is to take the matter seriously. Indeed, the country is lucky that it can learn from the mistakes of others whose experiences now form the body of knowledge for best practices.

At the very least an entity (a company or government) must establish what needs to be protected based on some security policy. The policy sets out governance and associated accountabilities in realizing security of the information. As well the entity must employ some best practice standards applicable to the practice of information protection and implement clear guidelines that realize the security of the information.

All people working for the entity must be trained to understand their roles in ensuring security of information. This starts with leadership, followed by everyone else. The required training must be commensurate with the roles of the people. It follows that technical people that install and maintain systems must have deep technical knowledge of security of the systems.

Like any live systems and processes, systems must be continually audited and any exposures fixed in a timely manner. Indeed, there must be ongoing monitoring for security violations (regardless of their magnitude and impact) and with necessary appropriate response. Incident management processes must be part of the security DNA of any enterprise.

For systems of interest to the public, a communication plan is always necessary. It is important that entities (be they public or private) continually keep stakeholders informed of breaches and assure the stakeholders that things are under control.

...

All this will not happen in a vacuum and required leadership. Today, our government has no designate information protection czar. Few companies have established the role of chief information security officer.

This leader would be a person with mandate for protection of an entity's (government or private company) information assets. This leader would ensure there is a framework that assures the protection of information, with proper processes, and trained people assigned appropriate responsibilities; the right people in the right place.

...

The Internet presents opportunities for government and private sector in Kenya. The country landed cables even as it was not prepared for consequences of such connectivity. For instance, no information protection framework was in place. Information protection leadership is yet to be established, which leaves a situation where we have technical and non-technical players in the Internet space that are not prepared. It is akin to sending an untrained person to drive on the super highway, oblivious of rules of the road.

It isn't too late but the urgency of the matter suggests prompt action.

© 2012 Matunda Nyanchama

*Dr Nyanchama is an information security professional, he is the director and principal consultants at Agano Consulting Inc with offices in Canada and Kenya. He can be reached at [mnyanchama@aganoconsulting.com](mailto:mnyanchama@aganoconsulting.com).*