Promoting a Culture of Cybersecurity : Zimbabwean Experience

Nicholas Ngoma

Postal and Telecommunications Regulatory Authority of Zimbabwe.

International Telecommunication Union

25th – 28th August, 2008 Lusaka, Zambia

Points to note

- *ICT is becoming the most powerful tool of day to day operations and functions of societies.*
- *Technologies are converging and there is widespread use of ICTs.*
- *Connections across national borders are increasing,*
- *Stakeholders and participants who develop, provide, service and use ICTs need to understand cybersecurity issues.*
- *Appropriate action must be taken to protect ICT networks.*
- *Government in leadership role in promoting Culture of Cybersecurity and supporting the efforts by other participants.*

Background

- As in many other countries worldwide, Zimbabwe stands no exception to the **influx of development triggered by ICTs**. In order to be abreast with these developments, it has become necessary for the country to **empower all sectors**, through Government initiatives, with enough knowledge on the use of ICTs. This has also prompted the Government to look into ways of protecting the nation from crimes triggered by this influx.
- Thus a **national strategy in promoting cyber security** has been spearheaded by the Government.
- Therefore all concerned **stakeholders in the industries** were made to comply with the laws meant to curb cyber crimes.

ICT enabled Society

- The government has embarked on a drive to **bring communication** to the doors of many in Zimbabwe through computerization of schools and communities.
- This is encouraging **communities and schools** to join the global village. Unfortunately, it is also a chance for opportunistic hackers to commit cyber crimes through stealing vital information from these communities.
- **Personal information and record holding communities** e.g. government institutions and government financial houses, are the most vulnerable since they are not adequately armed to deal with consequences of attacks.
- To date, many such communities are faced with a dilemma as to how to proceed without the **risk of being attacked** by destructive criminal activities.

Convergence of technologies and cross border connections.

- Like any other nationalities, Zimbabwe is relying much on information offered on global villages for all aspect of day to day operation i.e. learning, developments, etc.
- These include internet communication on both computers and cell phones through **GPRS and WAP**, online shopping by the use of credit cards, online banking etc.
- These developments **demand storage** of records and personal information.
- There is therefore a **risk of this information** being stolen in transit and therefore the need for protection against these attacks.
- There is no 100% guarantee in some institutions where these records are kept.
- This is the same case with single players (**home users**) who just register with operators to be connected to the village yet are not aware of the risks.

Stakeholder awareness

- The government of Zimbabwe, having noted that one side was covered while the other was left unattended, found themselves with a dilemma as to how they could protect these communities.
- A way forward was paved by the signing of a bill meant to both curb the use of ICTs and protection of the flow of information within the boundaries of Zimbabwe.
- The bill, known as **Interception of Communication Act [Chapter 11:20]**, came into effect in 2007. It seeks to monitor communication in the course of their transmission through ICT networks in Zimbabwe, and provide the establishment of a monitoring centre.
- The monitoring centre is yet to be enforced in the form of a **Single International Gateway**.
- The government therefore is in a process of holding **forums and workshops** with all stakeholders to enlighten them of the dangers and possible damage they may suffer.
- Also awareness programs in form of seminars are being run in collaboration with higher institutes of learning.

Implementation of programme

- The programme is to be put into effect in other sectors.
- The government in an effort to make its easier to the industry had decided that only main operators should install concerned equipment used to control and curb crimes of this nature.
- **The banking sector:** Heeded the government call to have systems well secured. The transfer system currently used in Zimbabwe is so far well protected and secure as up to now not a slight incident was experienced since its inception.
- The main obstacle to this programme is scarcity of funds allocations to the involved sectors as equipment needed maybe out of reach of those affected.

Challenges and solutions

- **Shortage of funds to pay for the system**: This challenge faced by some sectors if not all, e.g. schools, remote communities and some government sectors are not fully funded to cater for the development.
- **Threat to the whole system:** An attack by ICT threats like hackers, viruses and spasm may destroy unprotected establishments may end up transmitting itself to others through e-mail communications. E.g. Zimpapers, Fingaz were recently attacked by the hacking criminal group.
- **Lack of educational continuity programmes**: Engagement of local communities in a frequent awareness programme to make sure they know of the dangers and ways to protect themselves.
- The other challenge is from **GRPS and WAP** users as insufficient protection may damage both the cell phones and computers used in surfing the internet.
- The **government of Zimbabwe** is thus making it mandatory for all operators to make sure enough protection is installed to protect the nation from cyber crimes. Thus putting the burden on the operators.

References

- Government of Zimbabwe: *Interception of Communications Act [Chapter 11:20] No. 6/2007.*
- OECD "*Guideline on the Security of information Systems and Network: Towards a Culture of Security" [2000].*