ITU Regional Cybersecurity Forum for Eastern and Southern Africa

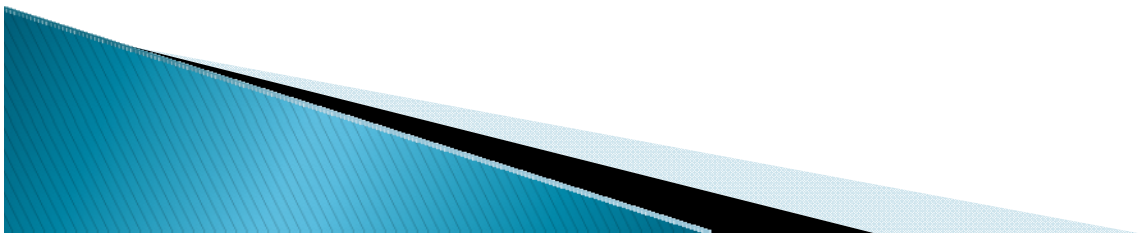
25th – 28th August 2008
Chisamba, Zambia

Cybersecurity in Zambia

Garry Mukelabai
Communications Authority Zambia

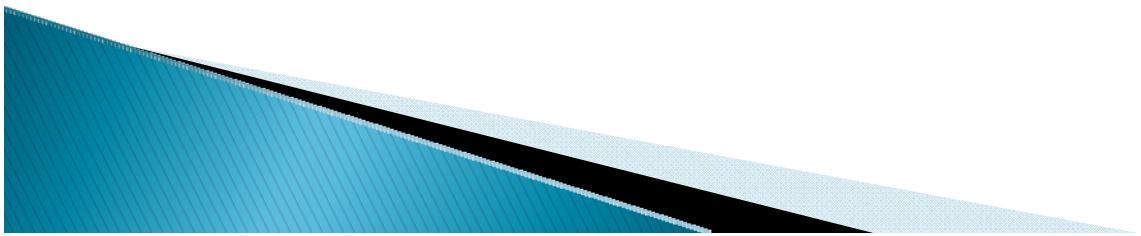
Contents

- ICT in Zambia.
- Current and Future Legislations.
- Way Forward ?



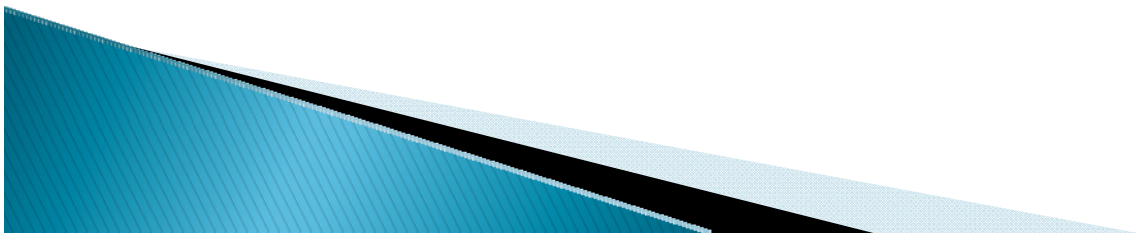
ICT in Zambia

- Pop 12 million.
- Zambia pioneers of internet in region.
- Over 10 Internet Service Providers
- Internet subscribers 16, 830 = 0.144 per 100
- PSTN subscribers 91,789 = 0.784 per 100
- Mobile subscribers 2,639,026 = 22.539 per 100
- (2007 figures)



Challenges to ICT growth

- High Cost of Access
  - Hardware
  - Software
- Poor Infrastructure
  - Concentrated along line of rail
  - Mobile phone has better penetration
- Poor Awareness
  - Users,
  - Security Issues
- Lack of Skills
  - End User, Professionals

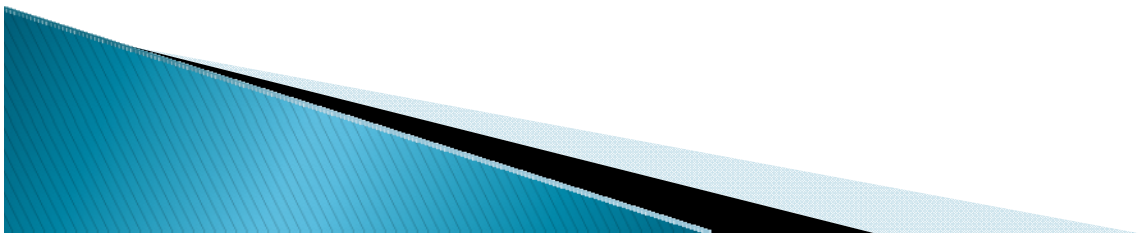


Cybersecurity in Zambia;

- Computer Misuse Act 2004 in place. Inadequate.
- ICT Policy March 2007
- ICT Bill in parliament being reviewed.
- ICT Security Bill being drafted
- E-signature Law being drafted.
- Inadequately trained judiciary and law enforcement.

Computer Misuse Act 2004

- Zambia has acknowledged the need for legislation of the use of cyberspace and this was brought to the fore with heavy lobbying by the banking sector with help of Computer Society leading to a Cybersecurity law the computer misuse act that was passed in 2004. "*However, critics are concerned that the law, if adopted, could be used to curb access to the internet.*
- The bill was passed quickly through parliament without much debate due to a suspected case of lack of understanding.

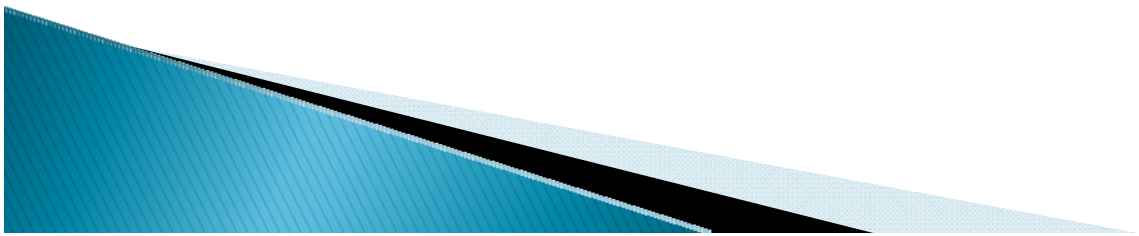


Computer Misuse Act 2004

- *Unauthorised access to computer program or data*
- *Access with intent to commit or facilitate commission of offence*
- *Unauthorised modification of computer program or data*
- *Unauthorised use or interception of computer service*
- *Unauthorised obstruction of use of computer*
- *Unauthorised disclosure of access code*
- *Enhanced punishment for offences involving protected computers*
- *Unauthorised receiving or giving access to computer program or data*
- *Causing a computer to cease to function*
- *Omission to introduce, record or store data*
- *Offences by body corporate*

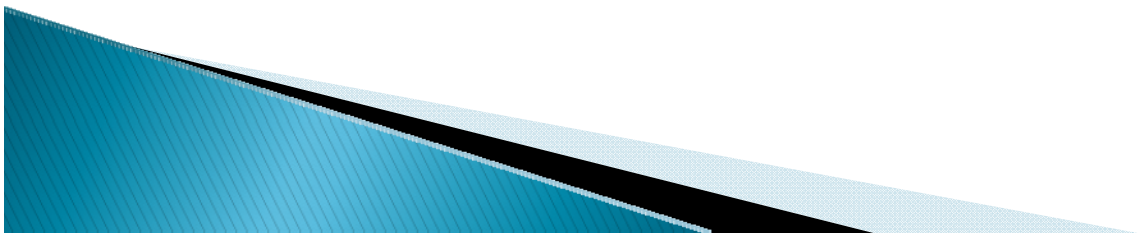
ICT Bill

- Backs the ICT Policy
- Radio and Telecoms
  - Radio Communications Act
  - Telecommunications Act



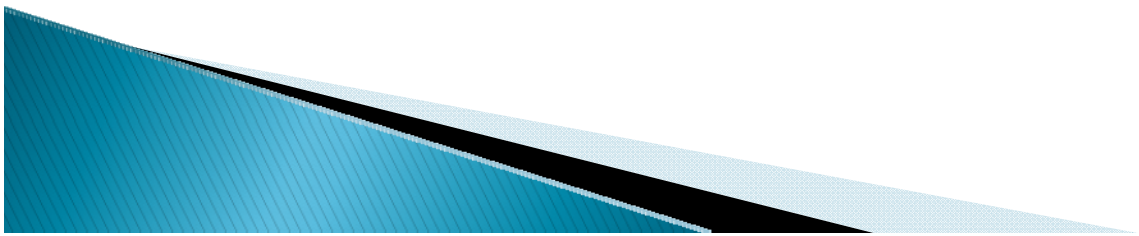
ICT Securities Bill

- Deals more with interception and monitoring.
  - Telephone records
  - User Details
- Deals with encryption up to any length
  - But requires permission.
- Access to stored documents.
- Being Drafted



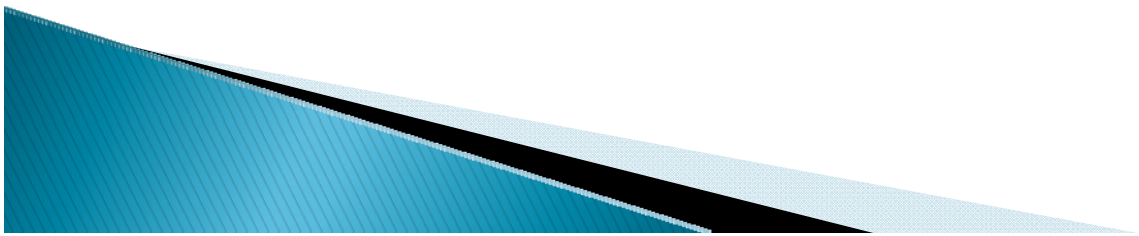
Electronic Transaction Bill

- E-signature
- Create enabling environment to allow
  - e-Commerce
  - e-Health
  - e-Banking
  - e-Government
  - Aned other related e- applications.



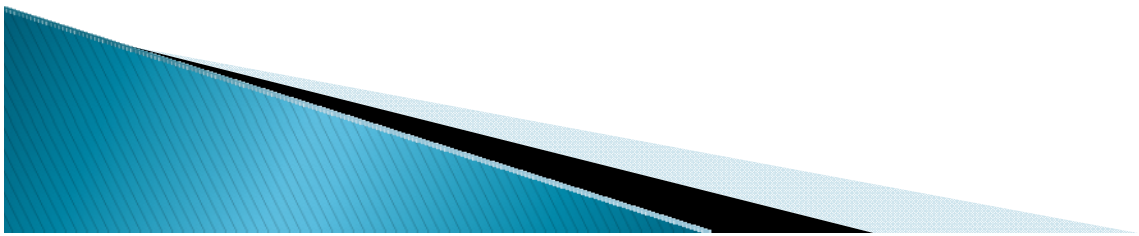
Others

- Mutual Legal Assistance Act –
  - Co-operation with other countries in curbing and prosecuting crime cross border.
- Anti Money Laundering Act –
  - Laundering including Cyber Related.
- Intellectual Property Rights Act
  - Copyright, Software Licensing
- Protection of Literacy and Artistic Works Act.
- Postal Services Bill



The Need

- Why is Cybersecurity important?
  - Critical sectors of a nation's economy today rely upon IP networks for transacting business, including energy, transportation, water, banking, agriculture and food, essential government services, etc.
  - To achieve maximum economic benefit from the use of IP networks, they need to be reliable, secure, and trusted.
  - Today, these networks, which were not originally designed with security in mind, face increasing threats from cyber attacks.

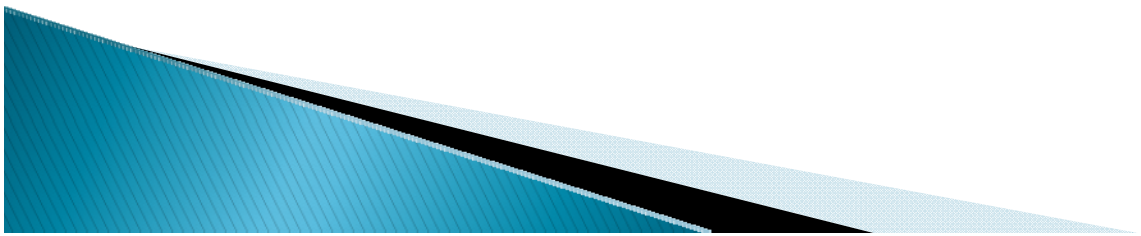


Statistics on Cyber Crime

- Zambia has very few recorded cases of cybercrime. A well published case involves the replacement of the portrait of the then republican President Fredrick Chiluba with a cartoon caricature. The offender was charged using the Telecommunication Act of 1994 that was created to regulate the telephone industry and Internet Service Providers and thus the charge failed to stick.
- At the time a bill was being drafted that was specifically for computer crime.
- The Police Service has received several reports of fraud cases of obtaining money by false pretence where offenders send mail to purporting to be rich heir and just needing a ‘small’ amount for money to pay commission or offering education scholarships for a small fee etc.

Fifth National Development Plan

- The government through the FNDP recognises and advocates for the use of ICT's for development as evidenced in the plan for computerisation of the Information Services through wide area networks and use of Management Information systems and again in Public Safety and Order on "computerisation" of crime prevention looks at the use of ICT database technologies to accurately record crime.



Vision 2030

- An information and knowledge-based society by 2030.

1. Increase connectivity to fibre optic (telecommunication infrastructure rollout) and other high capacity transmission technologies (networks) from 7 to 72 districts by 2010;
2. Increase the access to phones per 100 people (tele-density) from 0.9 to 8 by 2015 and to 50 by 2030; and
3. Increase access to ICT services such as Internet users from 35,000 in 2005 to 100,000 by 2015 and to 1,000,000 by 2030.

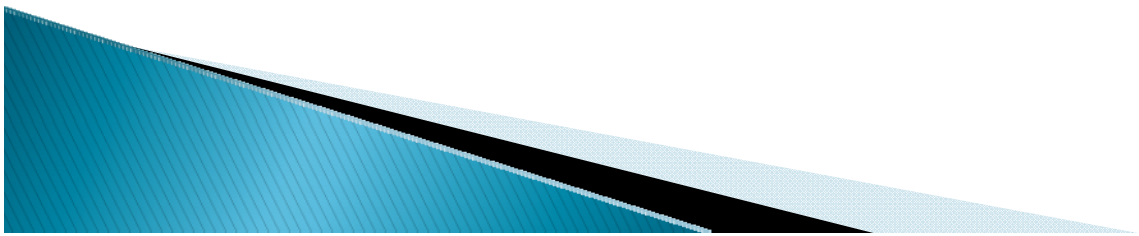
ICT Policy

- Launched March 2007 (PPP)

1. HUMAN RESOURCE
2. EDUCATION
3. ACCESS, MEDIA, CONTENT & CULTURE
4. ICT SECTOR
5. TELECOMMUNICATIONS INFRASTRUCTURE
6. E-GOVERNMENT
7. E-COMMERCE
8. AGRICULTURE
9. HEALTH
10. TOURISM, ENVIRONMENT & NATURAL RESOURCES
11. YOUTH & WOMEN
12. LEGAL & REGULATORY FRAMEWORK
13. SECURITY IN THE INFORMATION SOCIETY

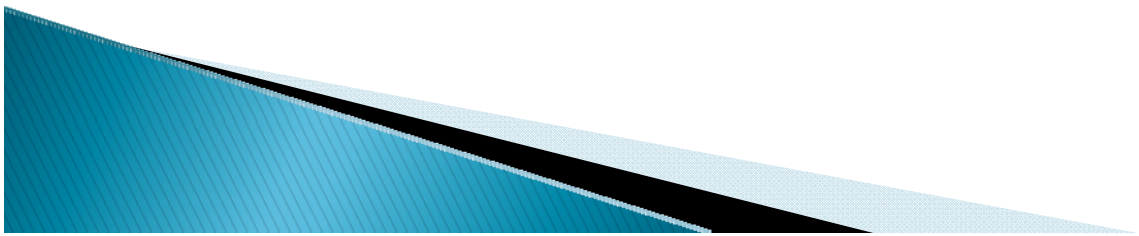
13 SECURITY IN THE INFORMATION SOCIETY

- In general, one of the greatest concerns in “connected” societies is security of information passing through networks and systems such as computers, financial transactions, health records etc. As Zambia embraces ICTs, more security concerns and abuse shall arise if no counter measures are put in place.



13 SECURITY IN THE INFORMATION SOCIETY

- (a) Security of government, public and private networks and communications systems in general; and in particular those systems carrying sensitive and critical data/information of great value to Government, businesses and individuals;
- (b) Protection of networks and information systems to guard against various types of malicious crimes and unauthorised access; safeguarding against undermining consumer confidence in online services including those based on E-Commerce, E-Government and E-Health systems;
- (c) Privacy of individuals, businesses and Government arising from connectivity to local, national and global networks.



WAY FORWARD

Awareness

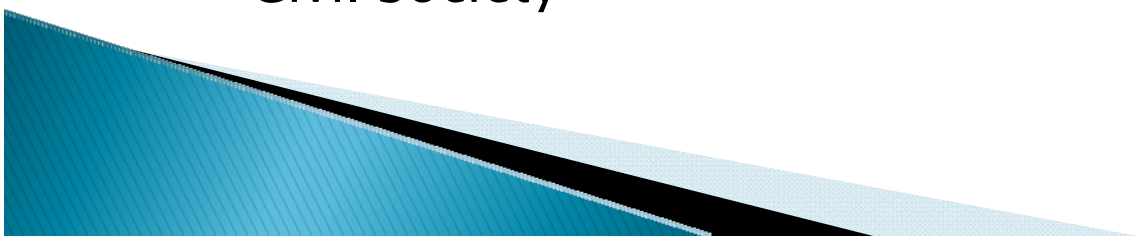
- "*Awareness to facilitate stakeholders' understanding of the nature and extent of their critical information infrastructures and the role each must play in protecting them.*"
- The stakeholders will include the government and its various arms, the
  - Legislative – Policy and Law Makers
  - Law Enforcement Agencies
  - Judiciary
  - Corporate, Individuals
  - Users, Public, Civil Society,
  - CAZ trained journalists, E-Brain monthly meetings, Computer Society, Media,

National Agency

- A national cyber security agency needs to be created that will oversee the running of the various facets of the topic. Such as
  - Incidence Response
  - Critical Infrastructure Information Protection
  - National Cooperation
  - Regional Cooperation
  - Training and Awareness
  - Security Audit
  - Currently – Min Comms and Transport are spearheading this activity

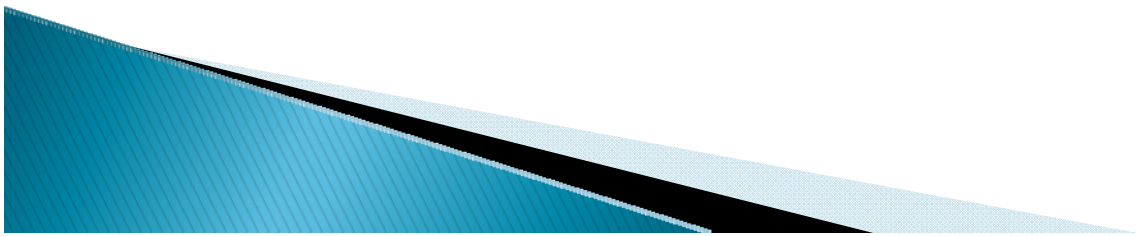
Stakeholders

- Security Wings
  - ZP, ZAF and Others
- Government and its wings
  - Ministry of Justice
  - Ministry of Communications and Transport
  - Ministry of Finance and National Planning
  - Bank of Zambia,
  - Regulators
- Business and Associations
  - Internet Service Providers, ISPAZ
  - Mobile Operators
  - Other ICT Service and Product Companies
  - Banks or Bankers Association
  - Ebrain, Computer Society of Zambia
- Academia
- Civil Society



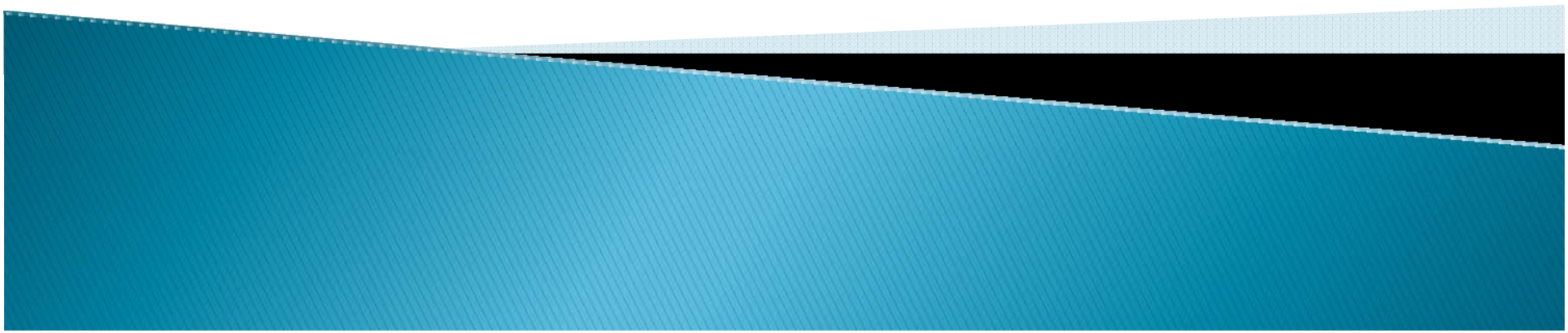
Regional Cooperation

- Cybercrime is quite often perpetuated across national boundaries. It is therefore important that nations co-operate and harmonise as many of their cybercrime legislations as possible to be able extradite offenders from one to another.
- Dual Criminality refers to a situation that requires that a crime be recognised in both countries before they can co-operate.



Thank You

gmukelabai@caz.zm



Glossary of terms used

- ICT Information and Telecommunication Technology
- ITU International Telecommunication Union
- ITU-D ITU Development Sector
- ITU-R ITU Radiocommunication Sector
- ITU-T ITU Telecommunication Standardization Sector
- PP-06 ITU Plenipotentiary Conference 2006
- SG Study Group
- TSAG Telecommunication Standardization Advisory Group
- WP Working Party
- WSIS World Summit on the Information Society
- WTSA World Telecommunication Standardization Assembly
- ZP – Zambia Police
- ZAF –Zambia Airforce
- ISP – Internet Service Provider
- PSTN – Public Switched Telephone Network
- SADC – Southern Africa Development Community