Cyber Regulatory Framework in Zimbabwe

Tichafa Rixon Mujuru
Postal and Telecommunications Regulatory Authority of Zimbabwe (POTRAZ)
2. Current legal framework
3. Proposed Framework (Cyber Bills)
4. Child Online Protection
Cyber Risk: The Growing Threat
Cyber Risk: The Growing Threat

- Technological developments
• Technological advancement
• Mobile penetration rose from 58.4% in 2010 to 95% in 2014
• Internet penetration rate escalated from 4.8% in 2010 to 45% in 2015
• A lot of internet subscribers access internet services through their mobile phones
• New services ushered in using of mobile broadband
  ✓ E-commerce
  ✓ Credit card payments
  ✓ E-banking
  ✓ Social media
  ✓ E-mail
  ✓ Mobile payments
  ✓ E-health
  ✓ E-agriculture
  ✓ E-learning
Internet Penetration

Active mobile penetration 95%
Internet penetration rate - 45.1%

Growth in internet subscribers

<table>
<thead>
<tr>
<th>Year</th>
<th>Internet Penetration Rate %</th>
</tr>
</thead>
<tbody>
<tr>
<td>2010</td>
<td>4.8%</td>
</tr>
<tr>
<td>2011</td>
<td>15.1%</td>
</tr>
<tr>
<td>2012</td>
<td>30.2%</td>
</tr>
<tr>
<td>2013</td>
<td>41.9%</td>
</tr>
<tr>
<td>2014</td>
<td>44.3%</td>
</tr>
<tr>
<td>2015</td>
<td>45.1%</td>
</tr>
</tbody>
</table>
Increased use of technology = increased risk of cybercrime

• Leading to;
  - Business disruptions
  - Online scams
  - Theft from business
  - Theft of data
  - Identity theft
Current Legal Framework

- Cybercriminal law in Zimbabwe is provided for mainly in Chapter VIII of the Criminal Law (Codification and Reform) Act [Chapter 9:23] (hereinafter referred to as the Code) enacted in 2004.

- This whole chapter (Sections 162-168 of the Code) provide for computer related crimes (often collectively described as ‘cybercrime’).

- Other statutes providing for cybercrime related offences are the Interception of Communications Act [Chapter 11:20] and the Postal and Telecommunications Act [Chapter 12:05]
Provisions of the Code

Chapter VIII of the Criminal Law (Codification and Reform) Act [Chapter 9:23]

Computer Related Crimes

- Section 163 - Unauthorised access to computers
- Section 164 - Deliberate introduction of computer virus into computer or computer network
- Section 165 - Unauthorised Manipulation of Computer data
- Section 167 - Unauthorised use of Credit and Debit Cards
- Section 168 - Unauthorised use of Passwords and Pin numbers

This law was enacted in 2004 and Zimbabwe like many other countries in the region is in the process of harmonising its cyber security laws with those of the region to increase international cooperation in the fight against cybercrime.
Current Efforts to Remedy the Situation

• Computer Crime and Cyber Crime Bill
• Data Protection Bill
• Electronic Transactions and Electronic Commerce Bill
• National ICT Policy
• Draft Child Online Protection Guidelines
Computer Crime and Cyber Crime Bill

• Crafted along the provisions of the Draft ICT Policy and the SADC Computer Crime and Cyber Crime Model law
• The main objectives of the Bill are;
  ✓ to provide a legal framework for the criminalisation of computer and network related offences.
  ✓ to criminalize certain illegal content in line with regional and international best practices,
  ✓ provide the necessary specific procedural instruments for the investigation of such offences and define the liability of service providers.

Provisions

The Bill is divided into 6 parts - Preliminary matters, specific offences, jurisdiction, admissibility of evidence, procedure and liability of service providers.
• Bill avoids over-legislating and facilitates both technological advancements and new and innovative developments in fighting cybercrime.
All offences established in this Bill, require that offender carries out the offences intentionally.

“person who intentionally, without lawful excuse or justification or in excess of a lawful excuse or justification...”

Nature of crime
Types of offences – three categories
- Offences against confidentiality, integrity and availability of computer data and systems
- Content related offences
- Computer related offences
Offences Against the Confidentiality, Integrity and Availability of Computer Data and Systems

Offences in this category are directed against at least one of the three key principles of cyber security (confidentiality, integrity and availability).

Most commonly occurring offences included in this category include:

- Espionage – illegal data acquisition –
- Illegal interception
- Data interference
- System interference
- Illegal access (hacking, cracking) e.g. breaking of password-protected sites, circumventing password protection on computer system – usually used to commit further crimes, e.g. data espionage, data manipulation or Denial-of-Service (DoS) attacks
Offences cont’d

Content-related offences –
• content considered illegal, including;
  ✓ Child pornography
  ✓ Racism and hate speech
  ✓ Spam
  ✓ Violation of Intellectual Property rights.

Computer-related offences
• category covers a number of offences that are committed through the use of a computer system including:
  ✓ computer-related fraud,
  ✓ computer-related forgery,
  ✓ illegal access,
  ✓ identity theft,
  ✓ harassment utilising means of electronic communications….

Combination of offences
category covers various terms used to describe complex scams that combine a number of different offences.
Jurisdiction

Part III (Sections 25-26)

- provides procedures to determine jurisdiction of the criminal offences enumerated above.

- Jurisdiction territorial and extra-territorial (ship/aircraft registered in enacting country, citizen etc)

- Territorial jurisdiction applicable if:
  - Both the person attacking a computer system and the victim system are located within the same territory or country.
  - The computer system attacked is within its territory, even if the attacker is not.
  - ship/aircraft registered in Zimbabwe

- Extra-territorial jurisdiction applicable if:
  - a national commits an offence abroad, and the conduct is also an offence under the law of the state in which it was committed or the conduct has taken place outside the territorial jurisdiction of any State
Part IV. Electronic evidence –
- deals with admissibility of electronic evidence in court and incorporates by reference the law dealing with electronic transactions & communication
- The current rapid growth of technology advancement in the world has impacted the criminal law by facilitating the traditional crimes and creating cybercrimes.
- Admissibility of electronic evidence is important in the prosecution of cyber offences

Part V. Procedural law – Provides a set of procedural instruments necessary to investigate Cybercrime;
- identification of offenders and protection of the integrity of computer data during an investigation contains several inherently unique challenges for law enforcement authorities.
- Bill introduces new investigation instruments aimed at facilitating and gathering of evidence and investigation of computer related crimes,
- enables investigating officer to order production of computer data.
  ✓ use specific search and seizeure instruments related to digital evidence and computer technology.
- enable law enforcement to use sophisticated investigation instruments such as key-loggers and remote forensic software, to collect passwords used by suspect, or to identify connections used by suspect
Part VI.

Provides a Framework Regulating the liability of Internet Service Providers

The Bill sets out the limitation of liability of service providers in hosting, access provision, catching, hyperlinks provision and search engine providers.

• In cases where liability exists, the bill limit criminal responsibility of Access Providers with regard to offences committed by users of their service, if provider did not initiate transmission, did not select receiver and did not modify information contained in transmission.

• Also for the Hosting Provider, liability is limited by the Bill, in cases where the provider has no actual knowledge about the existence of illegal data or immediately removes them upon obtaining such knowledge.
Child Online Protection (COP)

• Internet safety messages need to be timely, age specific, culturally sensitive and match the values and laws of the society in which the child or young person lives.

• POTRAZ is working on draft COP Guidelines which identify three principal age groupings of young Internet users.

• These groupings broadly correspond with the key stages of development on a child’s journey to adulthood.

• Hence the guidelines can be seen as a ladder which takes the child through progressive phases.

• However, we cannot over-emphasise that every child is different and requires and deserves individual attention. One size does not fit all. Nothing should ever be assumed or taken for granted.
The COP Initiative

  - Guidelines for 5-7 Years old
  - Guidelines for 8-12 Years old
  - Guidelines for 13 years and above
- Guidelines for Parents, Guardians, and Educators
- Guideline for Industry
- Guidelines for Policy Makers
General COP Guidelines for Children

- Meeting online friends offline
- Accepting Invitations / Friendships
- Reacting to inappropriate content or requests
- Handling personal concerns
- Making safe use of personal computer
- Personal online rights
Guidelines for the Age Group 5-7 Year Old

- Many young people in this age group will not be able to read or understand Guidelines on their own;
- Their usage should be **closely supervised at all times** by a parent or an adult person;
- **Filtering software or other technical measures** may also have a particularly useful role to play in supporting the use of the Internet by a child of this age;
- It would be wise to **consider limiting** such a young child’s potential access to the internet e.g. by constructing a list of safe web sites which are age appropriate;
- The aim is to provide this age group with the basics in Internet safety, etiquette and understanding.
Guidelines for the Age Group 8-12 Year old

- Netiquette
- Playing online games
- Bullying
- Personal digital footprint
- Offensive or illegal content
Guidelines for the age group 13 year old and above

- Harmful and illegal content
- Grooming
- Bullying
- Defending personal privacy
- Respecting copyright
- Online commerce
Thank You for your attention