INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA (ICASA) CYBERSECURITY PRESENTATION AT SAIGF

28th November 2018
AGENDA

1. State of Cybersecurity Globally
2. State of Cybersecurity in South Africa
   2.1 Policy landscape
   2.2 Legislation landscape and
   2.3 Regulations
The objective of the GCI as an initiative is to help countries identify areas for improvement in the field of cybersecurity, as well as to motivate them to take action to improve their ranking, thus helping raise the overall level of commitment to cybersecurity worldwide.

The five pillars of the ITU Global Cybersecurity Index (GCI)

1. **Legal**: Measured based on the existence of legal institutions and frameworks dealing with cybersecurity and cybercrime.

2. **Technical**: Measured based on the existence of technical institutions and frameworks dealing with cybersecurity.

3. **Organizational**: Measured based on the existence of policy coordination institutions and strategies for cybersecurity development at the national level.

4. **Capacity Building**: Measured based on the existence of research and development, education and training programmes; certified professionals and public sector agencies fostering capacity building.

5. **Cooperation**: Measured based on the existence of partnerships, cooperative frameworks and information sharing networks.
Current Landscape: ITU Global Cybersecurity Index (GCI)
ITU Global Cybersecurity Index (GCI)
Annex 1 – ITU Member States Global Cybersecurity Commitment Score By Region

<table>
<thead>
<tr>
<th>AFRICA Region</th>
<th>Score</th>
<th>Global Rank</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mauritius</td>
<td>0.830</td>
<td>6</td>
</tr>
<tr>
<td>Rwanda</td>
<td>0.602</td>
<td>36</td>
</tr>
<tr>
<td>Kenya</td>
<td>0.574</td>
<td>45</td>
</tr>
<tr>
<td>Nigeria</td>
<td>0.569</td>
<td>46</td>
</tr>
<tr>
<td>Uganda</td>
<td>0.536</td>
<td>50</td>
</tr>
<tr>
<td><strong>South Africa</strong></td>
<td>0.502</td>
<td>58</td>
</tr>
<tr>
<td>Botswana</td>
<td>0.430</td>
<td>69</td>
</tr>
</tbody>
</table>
Making South Africa a Global Leader in Harnessing ICTs for Socio-economic Development
02

Policy, Legislation & Regulations
Creating an Enabling Environment

Policy

South Africa has implemented a number of strategic and tactical interventions including the National Cybersecurity Policy Framework (NCPF) published on 4 December 2015, with the aim of:

1. Promoting a cybersecurity culture and demand compliance with minimum security standards;
2. Strengthening intelligence collection, investigations, prosecution and judicial processes, in respect of preventing and addressing cybercrime, cyber warfare, cyber terrorism and other cyber ills;
Creating an Enabling Environment

### Policy

<table>
<thead>
<tr>
<th>ROLE PLAYERS</th>
<th>ROLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>DTPS</td>
<td>The DTPS drafted the National Cybersecurity Policy Framework in 2012, and develop Cybersecurity Awareness Strategy to be implemented by all role players. To develop industry standards (with the assistance of ICASA and SABS), establish National Cyber security Advisory Council, establish Cyber security Hub, and sector specific CSIRTs.</td>
</tr>
<tr>
<td>National Cyber Security Advisory Council</td>
<td>To advise government on Cybersecurity policies.</td>
</tr>
<tr>
<td>Computer Security Incident Response Team (CSIRT)</td>
<td>Responsible for receiving, reviewing, and responding to computer security incident reports and activity.</td>
</tr>
<tr>
<td>Information regulator</td>
<td>A new regulator that has been created by the Protection of Personal Information Act (POPI). The Information Regulator has extensive powers to investigate and fine responsible parties. Data subjects will be able to complain to the Information Regulator and the Information Regulator will be able to take action on behalf of data subjects</td>
</tr>
<tr>
<td>Cyber hub/ CSIR</td>
<td>The hub is a link between the general public and the relevant institutions relating to the establishment of the sector CERTs</td>
</tr>
<tr>
<td>CSIR</td>
<td>Cybersecurity Innovation Centre</td>
</tr>
<tr>
<td>State Information Technology Agency (SITA)</td>
<td>Set standards for the interoperability of information systems and for a comprehensive information systems security environment for departments.</td>
</tr>
<tr>
<td>State Security Agency</td>
<td>Responsible for coordination, development and implementation of cyber security measures in the Republic as integral part of national security mandate. It must ensure that the Justice, Crime Prevention and Security (JCPS) cluster has requisite capacity in relation to National Cybersecurity Policy Framework (NCPF). It also host Cyber security Response Team and Cyber security Centre.</td>
</tr>
<tr>
<td>Department of Justice and Constitutional Development</td>
<td>To review various legislations governing cyberspace, harmonising and aligning them to the policy.</td>
</tr>
</tbody>
</table>
Creating an Enabling Environment

Legislation


- the right to privacy in section 14(d), which includes the right not to have the privacy of their communications infringed;

THE PROTECTION OF PERSONAL INFORMATION ACT, 2013 (ACT NO. 4 OF 2013) (“POPI”)

The Electronic Communications and Transaction Act, 2002 (Act No. 25 of 2002)

The Promotion of Access to Information Act, 2000 (Act No. 2 of 2000)

The Regulation of Interception of Communications and Provision of Communication-Related Information Act, 2002 (Act No. 70 of 2002)

Electronic Communications Act, 2005 (Act No. 36 of 2005)

Cybercrimes and Cybersecurity Bill
Regulators & Regulations

**Regulation**

**ICASA**

1. The mandate of ICASA ("the Authority") as stipulated in section 2(g) of the Electronic Communications Act of 2005 is to: "ensure information security and network reliability"

2. Section 36 (1) of the ECA states that "the Authority must prescribe standards for the performance and operation of any equipment or electronic communication facility, including radio apparatus."

3. Section 36 (2) further states that "such standards must be aimed at protecting the integrity of the electronic communications network."
Regulators & Regulations

Regulation

ICASA has since published on the “ROLE AND RESPONSIBILITIES OF THE INDEPENDENT COMMUNICATIONS AUTHORITY OF SOUTH AFRICA IN CYBERSECURITY”

This document seeks to solicit the inputs of all Stakeholders and interested parties on how they will like to see ICASA playing its role in this cybersecurity space on

The outcome of this process will guide ICASA on the next step
THE INFORMATION REGULATOR

The Information Regulator is, among others, empowered to monitor and enforce compliance by public and private bodies with the provisions of the POPIA. Once the relevant provisions of POPI come into effect, a person or business that is responsible for personal information (responsible party) will have to notify the Regulator as well as any parties whose personal information have been accessed or acquired by an unauthorised party.

The notification must, at the very least, contain the following information:

• A description of the possible consequences of the security compromise;
• A description of the measures taken or proposed to be taken by the responsible party to remedy the security breach;
• A recommendation of the measures that any party whose personal information was leaked in the security compromise should take in order to mitigate the possible adverse effects of the security compromise;
• The identity of the unauthorised person, if known, who accessed or acquired the personal information.
• The Information Regulator may also require the data breach to be publicised.
THANK YOU