CYBERSECURITY

OVERVIEW
Cyber Security – is a global challenge, policy makers worldwide are working hard to address security challenges of cyberspace. Cyberspace poses unique security challenges; global reach of ubiquitous networks, speed, jurisdictions & enforcement etc.

Cybercrime and cybersecurity are two issues that can hardly be separated. A multi-stakeholder approach is required to address the issues of cybersecurity and cybercrime.
BACKGROUND (Cont..)

ITU defines Cybersecurity as the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user’s assets. Organization and user’s assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user’s assets against relevant security risks in the cyber environment.

[ITU-T Rec. X.1205]
TYPICAL CYBER ATTACKS – Passive and Active Attacks

- Passive attack: Data Interception
- Active attack: Data fabrication, Data modification, Data destruction

Confidentiality, Availability, Integrity, Authenticity
TYPICAL CYBER ATTACKS

- **Denial-of-service (DoS) attack** - carried out by overloading system capacity, and preventing legitimate users.

- **Defacement attack** is carried out by replacing the victim’s web page with a wrong material e.g. pornographic, political.

- **Malware attacks** - is any program that can deliberately and unexpectedly interfere with the normal computer operation.

- **Spam** - bulk sending of unsolicited e-mail.

- **Phishing** - refers to an attack using mail programs to trick or coax web users into revealing sensitive information.
Cybercrime Ecosystem: Nodes and Flows

Source: ITU
ITU identified five pillars required to address cybersecurity:

1. Capacity Building
2. Technical and Procedural Measures
3. Organizational Structures
4. International Cooperation
5. Legal Measures
LEGAL AND POLICY FRAMEWORK

- Cybersecurity issues are not restricted by geography or national boundaries. A criminal located in one country can commit a cybercrime that produces its effects in a different country.

- It is very important cybersecurity legislations and policies are international and regionally harmonised.

- SADC have developed model laws for Cybercrime and Cybersecurity legislations.

- Various International Institutions are working Cybercrime and Cybersecurity such as ITU, UN, CTO, Budapest Cybercrime Convention, IMPACT etc.
LAW ENFORCEMENT ISSUES
There is a need to develop Comprehensive National Cybersecurity Strategy.

Create cybersecurity awareness and educate consumers.

Build capacity on cybersecurity and cybercrime issues.

Develop and review cybercrime legislation in order to ensure consumer protection.
THANK YOU

PULA