COMESA CYBER SECURITY PROGRAM

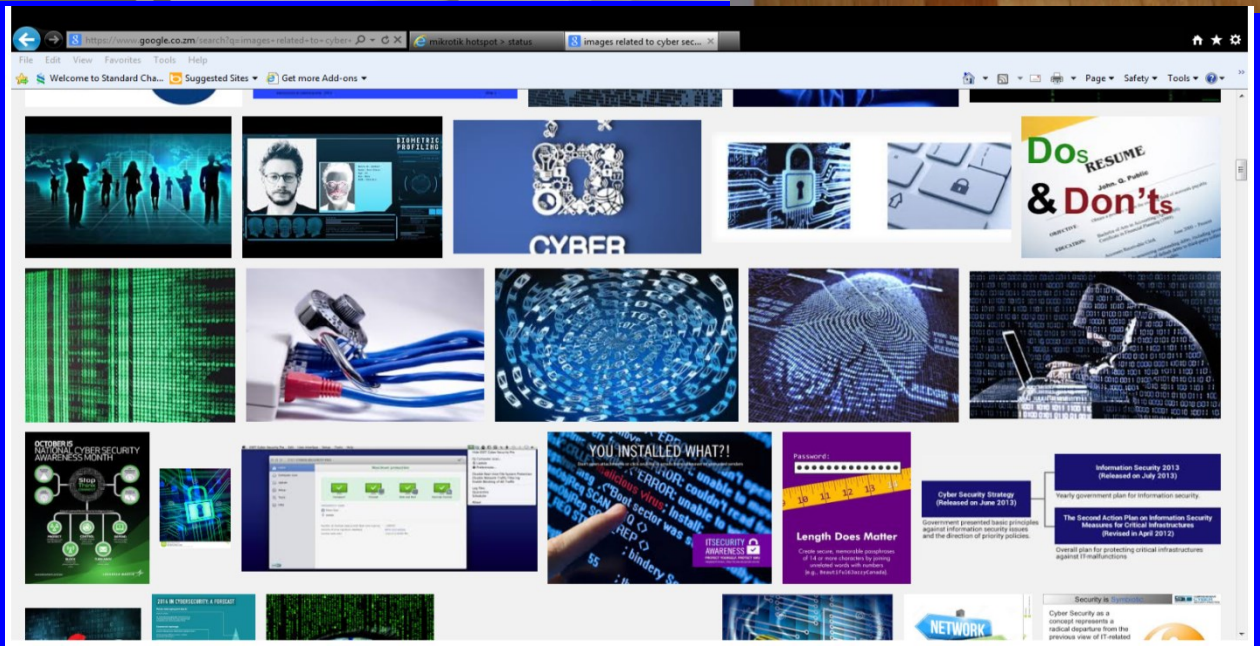
KHARTOUM, SUDAN

24-27 July 2016

CONTENT

- INTRODUCTION
- POLICY OBJECTIVES
- POLICY AND LEGISLATIVE PRINCIPLES
- CYBER SECURITY STRATEGY
- CHALLENGES AND OPPORTUNITIES
- CAPACITY BUILDING
- INTERNATIONAL AND REGIONAL COOPERATION
- ACTIONS

INTRODUCTION



INTRODUCTION

The main goal of cyber security policy is the maintenance of a secure, resilient and trusted electronic operating environment that supports governments security

Safe and reliable ICT is of fundamental importance for our prosperity and well-being and forms a catalyst for (further) sustainable economic growth.

In 2015, the British insurance company estimated that cyber attacks cost businesses as much as $400 billion a year. It will cost $2 trillion in 2019. Kenyan cybercrime cost is Sh15 billion in 2015. In Nigeria $450 million per year

POLICY OBJECTIVE

The main goal of these policy guidelines is to assist member countries in the development of a safe and secure cyberspace within the COMESA region which will facilitate and promote regional cooperation. Specific objectives are:

- Harmonizing the legal and regulatory frameworks for COMESA Member States which are aligned with international best practices;
- Facilitating the establishment of relevant structures in support of cyber security;
- Ensuring the reduction of cyber security threats and vulnerabilities;
- Coordinated local and international partnerships
- Continuous innovation, skills development and compliance

POLICY AND LEGISLATIVE PRINCIPLES

Trust: enhance the confidence of consumers, businesses and governments in the confidentiality, integrity and availability of the online environment

Innovation: maximize the ability of organizations to develop and adopt the widest possible choice of cutting edge cyber security solutions.

Protection: implement the security measures that are most appropriate to mitigating the specific risks faced by consumers, businesses and government agencies .

Standards:

Policy convergence: must recognize the borderless nature of the Internet, of the global economy and of cyber threats

POLICY AND LEGISLATIVE PRINCIPLES

Check user identity:
Develop acute situational awareness:
National Coordination:
Accreditation and Testing Services: promote the development and maintenance of good practice in testing and inspection and maintain a registration scheme for organisations that comply with that practice.
Information Security Assessment:
Cyber Defence:

POLICY AND LEGISLATIVE PRINCIPLES

System Vulnerability Analysis:
Defining and classifying network or system resources, Assigning relative levels of importance to the resources, Identifying potential threats to each resource, Developing a strategy to deal with the most serious potential problems first, Defining and implementing ways to minimize the consequences if an attack occurs.

Threat Analysis and Remediation:

Enterprise Information Security Architecture:

Cyber-Insurance: Information Assurance:

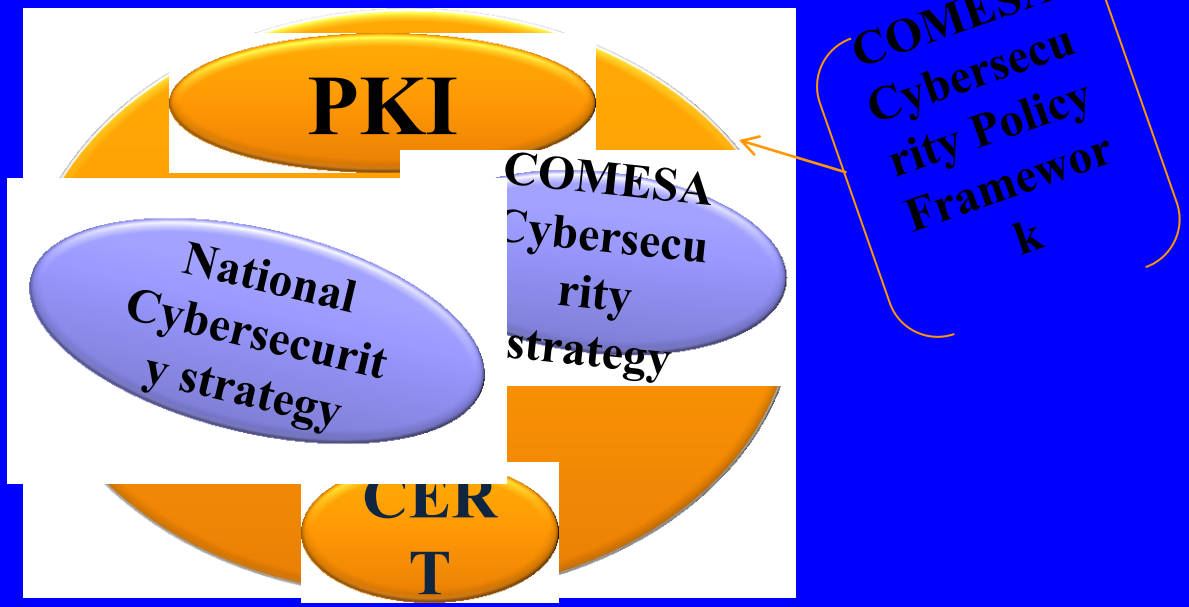
STRATEGY

Strategy is a roadmap allowing Governments departments and institutions to better define and coordinate their role in cyberspace policy and legal framework, to execute a specific way forward, and to plan for future implementation. The cybersecurity strategy should be aligned with the goals of the country and should be built to serve the states objectives

Reasons to establish a Cyber security Strategy:

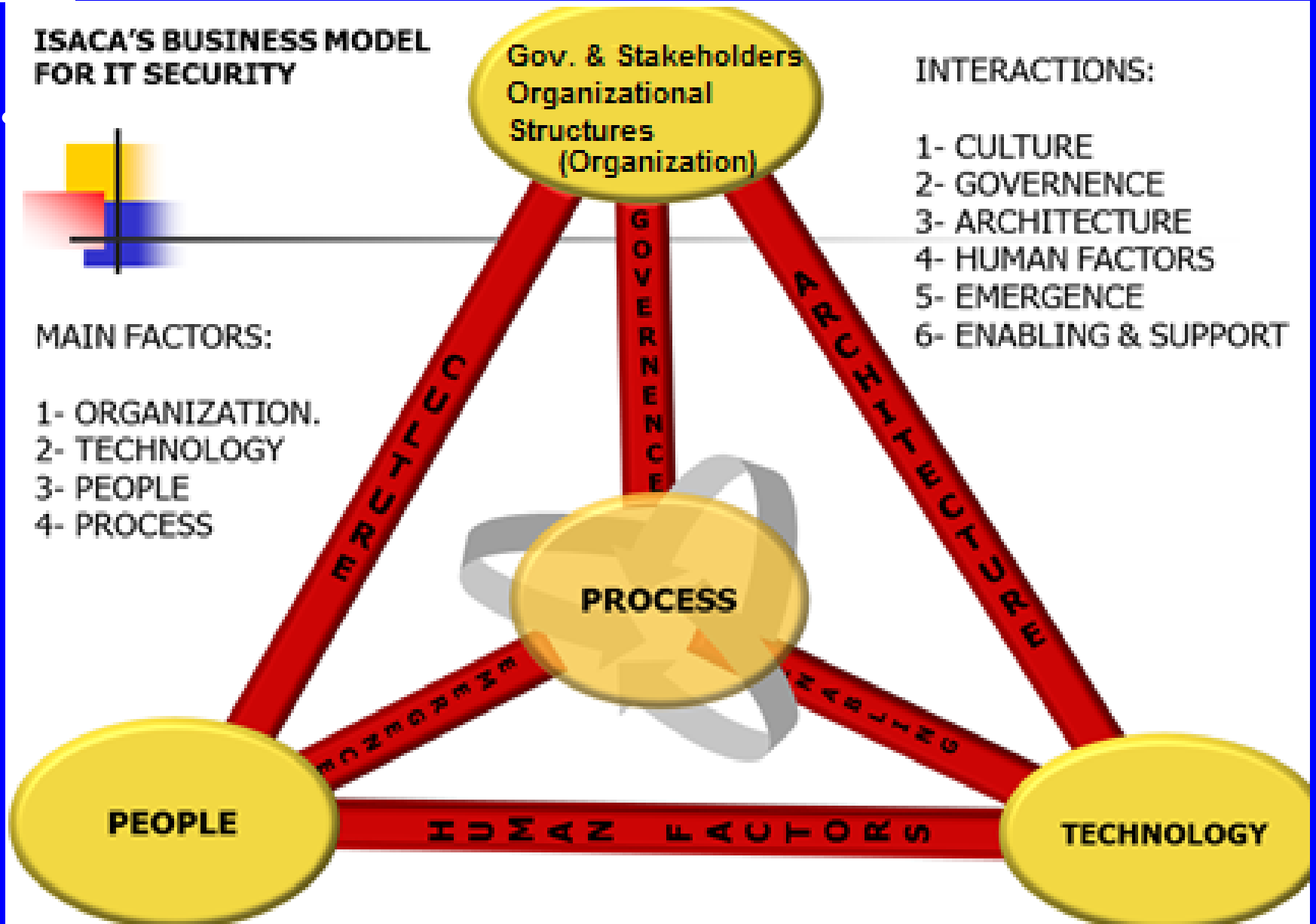
- Securing cyberspace,.
- Need for collaborative approach to Cyber security initiatives within the state, all stakeholders must be involved.
- Cyber security awareness and capacity building.
- Facilitate social-economic development.

STRATEGY
Purpose of the cybersecurity strategy model document



- Rationale for a cybersecurity strategy.
- Facilitate development of a national version of the cyber security strategy.
- Involvement of all stakeholders
- Establish a foundation for a COMESA cybersecurity strategy.

STRATEGY


ISACA'S BUSINESS MODEL FOR IT SECURITY
Gov. & Stakeholders Organizational Structures (Organization)
INTERACTIONS:
1- CULTURE
2- GOVERNENCE
3- ARCHITECTURE
4- HUMAN FACTORS
5- EMERGENCE
6- ENABLING & SUPPORT
MAIN FACTORS:
1- ORGANIZATION.
2- TECHNOLOGY
3- PEOPLE
4- PROCESS
GOVERNENCE
PROCESS
PEOPLE
TECHNOLOGY

STRATEGY: GOALS AND MEASURES

Goals and measures In order to reduce the vulnerability of cyberspace, the following strategic goals have been identified:

- establishment of a multilevel system of security measures;
- expanding expertise in and awareness of information security;
- adopting an appropriate regulatory framework to support the secure and extensive use of information systems;
- consolidating the position as one of the leading countries in international co-operative efforts to ensure cyber security.

STRATEGY
STAKEHOLDERS AND THEIR ROLES

- Legislators: To provide the legal framework.
- Constituents: To realize the importance of the cybersecurity initiative to their economic well-being.
- Judiciary and court system: Full capacity & awareness.
- Executive Institutions of Government responsible for the ICT: Drives the initiative (Compliance, Standards, Drafts Strategy).
- Research and Academia: Work on the basic research.
- Private sector companies in the cybersecurity industry: Capacity building & the know-how
- Telecom Critical Infrastructure Owners and Operators: Responsible for implementing strategy at the backbone

CHALLENGES

The COMESA region faces the following challenges:

- Lack of policy and legislation framework in most of Member States;
- establishment of national and regional CIRT and PKI
- Risk amount and eminence around member states' **Critical Information Infrastructure's (CII)** is high. There is minimum to no security on **CII**
- low literacy rates especially on Internet security awareness; ;
- exchange of information and tackling the crimes.
- Few forensic labs in the region

CHALLANGES

- non existence of central information security body to educate the layman around Internet security and other cyber security issues;
- Availability, reliability and affordability of users protection ;
- Freeware downloads offer no guarantees on functionality and do not provide support; and
- Lack of regional framework for cooperation, protection,
- Rapid advances in deployment of new technologies (NGN standards, LTE etc.)
- Mapping legal and regulatory instruments with existing and new technologies

OPPORTUNITIES

e implementation of the Policy Guidelines leading to a secure cyberspace will achieve the following benefits:

- Confidence and security in the use of ICTs by Government, business, society and the individual;
- Identification and protection of critical infrastructure;
- A safe and secure cyberspace;
- Secure environment for electronic communication and conducting electronic transactions;
- Economic growth and competitiveness of the Member States and the region;
- Reduction of cyber crime impact on the economy

CAPACITY BUILDING

- Training on Law enforcements, prosecutors, investigators, lawyers and judges.
- Training for CIRT experts;
- Training for PKI regulators and experts
- Raising the awareness of users,
- Study tour

INTERNATIONAL & REGIONAL COOPERATION

- cooperation is critical due to the borderless nature of the cyber security attacks
- achieving worldwide moral condemnation of cyber attacks given their negative effects on people's lives and the functioning of society,
- Involvement in the development and implementation of regional and international cyber security policies
- developing co-operative networks in the field of cyber security and improving the functioning of such networks.
- Judiciary system

- **Internet Site: http://www.comesa.int**