IMPLEMENTATION OF A FRAMEWORK TO SUPPORT CYBERSECURITY AND INTERNET GOVERNANCE IN CAMEROON

Presented by:
Njei Check
Head, Audit Security Division,
ANTIC

Windhoek, 30th May 2017

SUMMARY

1. INTRODUCTION
2. COMMON THREATS FACED IN CAMEROON'S CYBERSPACE
3. SECURITY SOLUTIONS DEPLOYED TO SECURE CAMEROON'S CYBERSPACE
4. PERSPECTIVES
5. CONCLUSION

1. CONTEXT

1.1. ICT Development in Cameroon

❖The Government of Cameroon is committed to deploying ICT related solutions across government agencies and departments. Benefits of this effort include: greater efficiency, improved public services, reduced corruption and enhanced engagement with citizens.

❖In 2009, Cameroonian government put in place a framework which focuses on cybersecurity activities and considering cybersecurity risks as part of the country's risk management processes

❖Security related solutions are highly needed to protect citizens and government information systems in terms of ensuring information availability, integrity and confidentiality.

❖ Our Government has established a National Public Key Infrastructure (PKI), a Computer Incident Response Team (CIRT) and other cyber security solutions such as nationwide security audits of information systems.

❖The Government has also developed a legal and regulatory framework to help fight against cyber crimes.

1.2. Common security threats in Cameroon

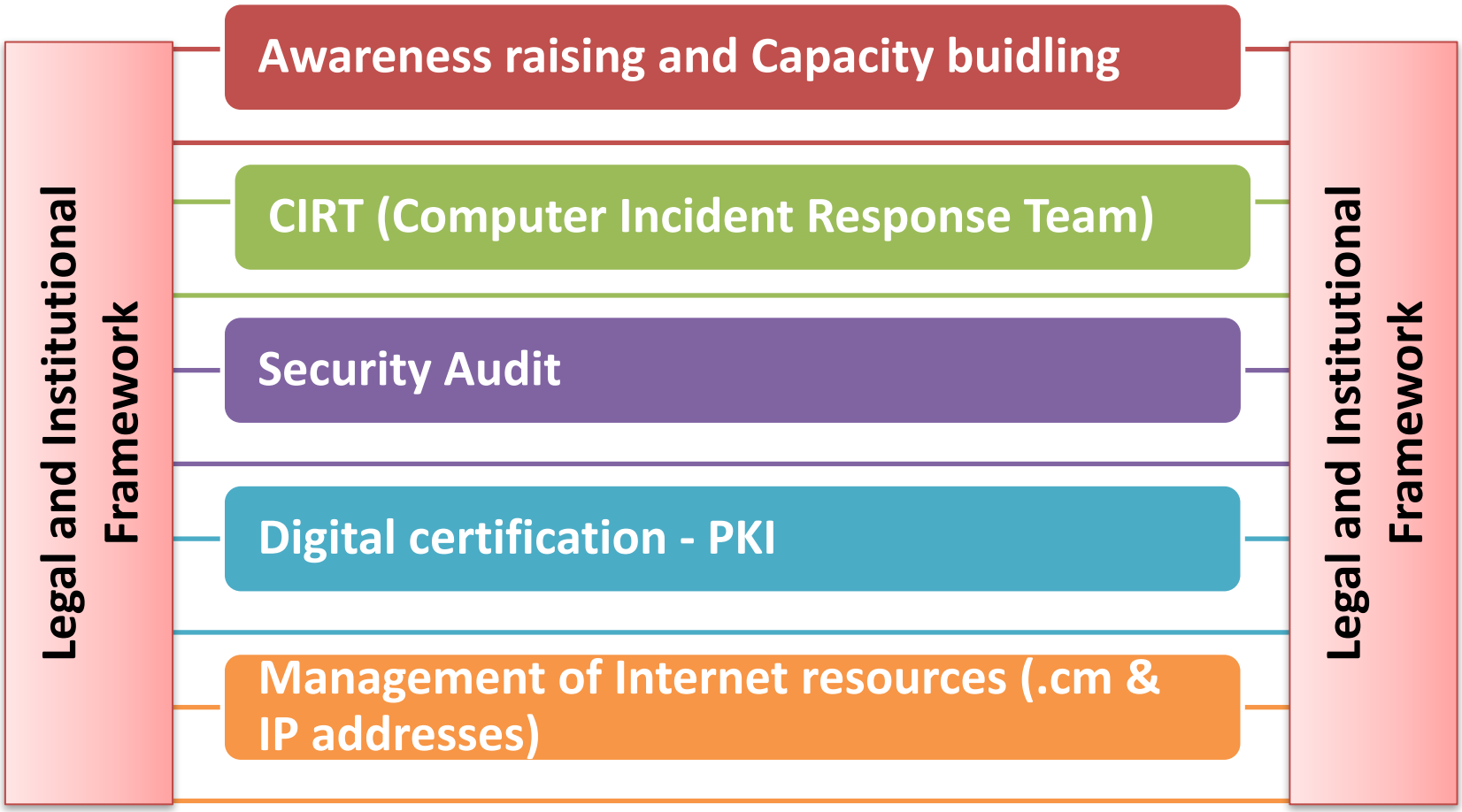
1. Scamming
2. Phishing
3. Skimming
4. Webdefacement
5. Hoax
6. Unlicensed software
7. Malware
8. SIMBOX

1. CONTEXT

1.3. Some statistics on cybersecurity in Cameroon (2012 – 2016)

- More than 8 Million USD loss incurred through scamming and phishing
- More than 7 Million USD loss incurred through skimming
- More than 300 cases of social network profiles spoofing and blackmail registered
- More than 400 thousand USD loss incurred through intrusion
- More than 25 million USD loss incurred through SIMBOX fraud
- 28 webdefacement attacks perpetrated against public administration websites
- More than 12814 vulnerabilities detected on public administration websites
- More than 150 requests related to cybercriminality received from INTERPOL and law enforcement
- **Global cybersecurity index: 0,4118 (5th in Africa and 15th world wide, ITU 2014)**

2. CAMEROON'S CYBERSECURITY & INTERNET GOVERNANCE FRAMEWORK



2. CAMEROON'S CYBERSECURITY & INTERNET GOVERNANCE FRAMEWORK

2.1. Legal and Institutional Framework

- Enactment of Law No. 2010/012 on cyber security and cyber crime which punishes cybercrimes such as intrusion into information systems, denial of service and privacy related attacks
- Enactment of Law No. 2010/013 of December 21, 2010 on electronic communications, which was subsequently amended by Law No. 2015/006 of April 20, 2015;
- Reorganization of ANTIC by Decree No. 2012/180 of April 10, 2012;
- Creation of a special fund to finance cyber security related projects.

2. CAMEROON'S CYBERSECURITY & INTERNET GOVERNANCE FRAMEWORK

2.2. Awareness raising and capacity building

- Development of best practice guidelines
- Organization of sensitization seminars
- Animate radio program dedicated to cybersecurity
- Creation of cybersecurity program in universities

2. CAMEROON'S CYBERSECURITY & INTERNET GOVERNANCE FRAMEWORK

2.3. CIRT

- Monitoring of critical IT infrastructures
- Issuing security bulletins and alerts
- Providing assistance to end user and companies in handling security incidents
- Developing cybersecurity related standards (policy, procedures)
- Digital Forensic investigations
- Establishing and maintaining partnerships with other CIRTs and security organizations.

2.4. Security audit

Analysis of critical information systems aimed at detecting vulnerabilities, evaluating risks and proposing measures to correct the vulnerabilities detected.

- Over 100 security audit missions carried out in both public and private organisations (2013 - 2016);
- Over 10 000 vulnerabilities detected (2013 - 2016);
- Improvement of ICT user's awarness on cybersecurity

2. CAMEROON'S CYBERSECURITY & INTERNET GOVERNANCE FRAMEWORK

2.5 Digital certification (operational , 2012)

Using Public Key Infrastructure (PKI) technology in securing automated processes

- Setting up of a Root Certification Authority
- Setting up of an accredited certification authority

Secured applications

- e-GUCE (GUCE)
- e-Procurement (MINMAP)
- e-Billing (ANTIC)

Ongoing

- Teledéclaration (CNPS)
- Teledéclaration (DGI)
- NEXUS (DGD)
- Driving license (MINT)
- PrideSoft (ARMP)

2. CAMEROON'S CYBERSECURITY & INTERNET GOVERNANCE FRAMEWORK

2.6. Management of Internet resources

- Development of an IPv6 migration strategy
- Development of .CM chart and an IP address chart
- Setting up of a national .CM mail service platform
- Implementation of DNSSEC
- Setting up of two IXP
- National campaign of Telcom subscriber identification
- Building of Whois platform for public IP addresses
- Organisation of national Internet Governance Forum (annually)

3. PERSPECTIVES

- Improve on the sensitization and capacity building
- Reinforce the national CIRT
- Construct a backup for the national PKI
- Construct a national government datacenter
- International recognition of SSL certificates issued by Cameroon's PKI
- Accredit private companies to carry out security audits
- Improve on the development of local content
- Reinforce the legal and regulatory framework
- Promote the migration from IPv4 to IPv6

4. CONCLUSION

In the last few years, the digital economy, as a catalyst for innovation and competitiveness, has become an important lever for economic development. As an illustration, a recent report of the world bank advocates that an increase of 10% in broadband usage can lead to an increase of 2% in the GDP.

Unfortunately, the development of digital economy is jeopardized by cybercriminality that thrives on the virtuality of the cyberspace and seriously damaging the trust within the cyberspace.

Therefore, to reach the expectations of digital economy, it is imperious to reinforce the security of our cyberespace.

Thank you for your kind attention

Contact: njei.check@antic.cm