BUILDING NATIONAL CYBERSECURITY CAPACITY IN NIGERIA: THE JOURNEY SO FAR

**Presenter** – M.U. Maska, Director of Cybersecurity, Office of the National Security Adviser, Nigeria.

u.maska@cert.gov.ng
info@cert.gov.ng
+234-803-586-6773.

Regional Cybersecurity Forum for Africa and Arab States, Tunis 2009.
Introduction
Cybersecurity Issues
Steps Taken by Nigerian Government
Objectives of National Cybersecurity Initiative (NCI)
Nigerian Cybercrime Working Group (NCWG)
Directorate of Cybersecurity (DOC)
Activities of DOC
Challenges
Nigeria has population of over 150 Million.
Youth mostly Educated to High school Constitute over 40% of the Population.
Key Economic Activities are in areas Oil & Gas, Banking, Agriculture and Manufacturing industries. It is the Economic Hub of the West African sub region.
Advent of Internet in Nigeria was in the mid 90s, then used mostly by Multinational firms for Legitimate Business.
Service was only available through the Government owned Nigerian Telecommunication Company.
Subscription was very expensive and usage limited.

During the Deregulation of Telecom Sector of late 1990s, few more private ISPs were licensed and access became less expensive.

With the proliferation of ISPs and Cybercafés in the country Fraudsters started using the Internet, instead of the Regular Mails and Fax.

Government became Alarmed with the Misuse of Cyberspace by the Fraudsters.
Cybersecurity Issues In Nigeria

- Website Cloning (e.g. Banks, Telecomms etc.)
- Phishing (e.g. Username, Password, Card Info)
- E-commerce fraud (e.g. in Ebay Transaction)
- Credit card fraud (e.g. Card scheming, Generating Card Info etc.)
- Advance Fee Fraud (a.k.a 419)
  - Re-shipping fraud
  - Romance fraud
  - Inheritance fraud
  - Lottery scam
  - Crude oil sales scam etc.
Steps Taken by the Nigerian Government

- In 2003, the President of Nigeria set up a Committee to Investigate the Activities of these fraudsters on Cyberspace.
- Also in 2003, the Government set up the Economic and Financial Crimes Commission (EFCC) to Tackle the menace of Corruption, Advance Fee Fraud, and Money laundering.
- The Presidential Committee came up with the National Cybersecurity Initiative (NCI), which has the following objectives:
Objectives of National Cybersecurity Initiative (NCI)

- Public Enlightenment of the Nigerian Populace on the nature and danger of Cybercrime.
- Criminalization through new Legislation of all on-line vices.
- Institutional Capacity Building across Law Enforcement Agencies to extend Statutory Functions on Cybercrime related issues.
Establishment of Legal and Technical Framework to Secure Computer Systems and Networks, and Protect Critical Information Infrastructure for the country.

Creation of a platform for public–private stakeholders collaboration to set Guidelines and Standards for Cybersecurity in Nigeria.

Building International Law Enforcement Cooperation and Collaboration with other Agencies Worldwide to enable Nigeria tackle the menace of Cybercrime.
In 2004 Government then set up the Nigeria Cybercrime Working Group (NCWG) to realize the Objectives of NCI.

NCWG team was made up of Government officials, ICT related Ministries and Departments as well as Law Enforcement Agencies.

It was mandated to implement the NCI Objectives within two years.
NCWG conducted Public Enlightenment on Cybercrime successfully among Public and Private Institutions in Nigeria.

Drafted Computer Security and Critical Information Infrastructure Protection Bill.

Nigeria through the EFCC joined the G8 – 24/7 Network of High Tech Crime Group (US Dept of Justice).

A number of cases on Cybercrime are now being Investigated and Prosecuted in Nigeria (e.g. Operation Cyberstorm)
Directorate of Cybersecurity (DOC)

- In 2006 Directorate of Cybersecurity under the Office of the National Security Adviser was created to sustain the Good work of NCWG.
- DOC is presently the apex body that Coordinates the Activities of Cybersecurity in Nigeria.
- Its Mandate is the implementation of the NCI objectives.
Activities of DOC

- Develop a framework for National Computer Emergency Response Team (CERT), [www.cert.gov.ng](http://www.cert.gov.ng).
- Establishing collaboration with CERTs around the world.
- Establishing a National Computer Forensic Laboratory and Coordinating the training and utilization of the facility by all Law Enforcement Agencies in Nigeria.
Activities of DOC

- Public awareness campaign
  - NGO’s
  - National Assembly
  - Law enforcement agencies

- Sponsoring passage of ‘The computer Security and Critical Information Infrastructure Protection Bill’ in the National Assembly.
Challenges

- Cybercrimes are transnational and perpetrators continue to utilize legislative loopholes, intelligence gaps and jurisdictional issues to their advantage.
- Passage of the Bill and Amendment of Nigerian Evidence Act.
- Acquisition of modern technological tools to Prevent, Monitor and Investigate Cybercrime which is dynamic.
- Near absence of single Internet Gateway.
- Training.
Thank you for listening