Framework for Cybersecurity in Nigeria

Basil Udotai, Esq.,
Director & Head,
Directorate for Cybersecurity (DfC),
Office of the National Security Adviser, Nigeria
Praiamar Hotel, Praia, Cape Verde
Nov 27-29, 2007

Dual Role

- Moderator
- Speaker

What are the issues?

- Increasing Reliance on ICT – personal, business and Government;
- Gaps in Law Enforcement, Intelligence and National Security;
- Incentive for Public Sector Reform lacking;
- Private Sector Growth – creates a “hands off” attitude – Incentive not to lobby for reform; Business Model favors and supports current attitude;
- Regulator confused about proper role – network growth; penetration; no content regulation; FDI protection, etc
- Lack of CREATIVE Involvement on the part of the International Community – ITU proving to be a worthy exception – WBG needs to catch up

Creative Int'l Involvement?

- What would constitute creative international involvement in cybersecurity?
- When World Bank and other Development Partner Organizations begin to condition International Development Assistance and associated aids on the existence of a certain level of national framework on cybersecurity;
- Is there a precedent for this?

Of course, Corruption

- What is good for corruption is good for cybersecurity!

Typical Measures

- Policy: What do we need to promote; prohibit; prohibit and protect
- Law: cybercrime as strategy for cybersecurity; substantive and procedural law; criminalization of all undesirable activities occurring in the online environment and creating legal procedures for investigation, prosecution and conviction;
- Institutional Capacity Building: facilities and human capacity building all geared at ensuring that law enforcement and related mandates authorized by statute in the offline environment are migrated to the online environment as well;
- Public Private Partnership: most critical networks are now privately owned and managed around the world, fast becoming the case in Nigeria, ICT equipment manufacturers and solutions providers are all private; thus, the need to build consensus, agree on standards, rules and best practices for cybersecurity;
- Public Enlightenment: nature and impact of issues concerned;
- International Law Enforcement Cooperation: necessitated by the global domain of the network environment and the ability for criminal actions to occur anywhere and affect interests in other parts without limitation

What we have done

- Awareness – started with the Press and covered all crucial areas
- Legal Reforms; we have proposed relevant laws, especially the Draft Bill on Computer Security and Critical Information Infrastructure;
- Institutional Capacity Building; designed models for establishing relevant Units at Agencies (Cybercrime Units, law enforcement; and Computer Crime Prosecution Units, at the Office of the AGF, which can become a model for states; Digital Evidence Management System and Judicial Reform Project, focusing on new Court Rules and Training of officials for Electronic Evidence Handling
- Public Private collaboration; Govt-Industry Forum on Lawful Interception, proposed to be continuous under a permanent framework to be known as Nigerian Information Security Alliance (NISA); National CERT; starting with Sector-based CERTs in the financial sector to be followed by the Telecoms sector and so on;
- International Law Enforcement Cooperation – now member of the G8 24/7 Network, represented by EFCC, established broad based law enforcement relationship with many international law enforcement agencies, including the USA, UK, South Africa, etc.

Framework for Cybersecurity - Background

- The Tragedy of the Diplomat assassination in the Chez Republic;
- Presidential Committee on Illegal Online Activities
- Established in April 2004, following recommendations by the Presidential Committee on illegal online activities, Chaired by the National Security Adviser;
- It is an Inter-Agency body made up of all critical law enforcement, security, intelligence and ICT Agencies of government, plus major private organizations in the ICT sector;
- ToR include awareness and enlightenment programs targeting both public and private sector; building institutional consensus amongst existing Agencies, providing technical assistance to the National Assembly on Cybercrime and the Draft Bill; laying the groundwork for the computer crime enforcement and prosecution by relevant agencies; developing technical guidelines for industry on cybersecurity; and commencing relations with international law enforcement organizations – CCIPS (USA), NHTCC (UK), NPA (SA), for global law enforcement cooperation

Framework for Cybersecurity – Background 2

NCWG Structure and Management

- Economic and Financial Crimes Commission (EFCC),
- Nigeria Police Force (NPF);
- the National Security Adviser (NSA),
- the Nigerian Communications Commission (NCC);
- Department of State Services (DSS);
- National Intelligence Agency (NIA);
- Nigeria Computer Society (NCS);
- Nigeria Internet Group (NIG);
- Internet Services Providers' Association of Nigeria (ISPAN);
- National Information Technology Development Agency (NITDA), and
- Individual citizen representing public interest.
- 2 Chairmen - HMST and HAGF
- 1 Coordinator – General Council and Legal Adviser of NITDA

Framework for Cybersecurity – Status

- NCWG was given 2 years within which to complete its mandate;
- Tenure expired December 2006;
- Directorate for Cybersecurity (DfC), was created as a permanent autonomous body within the Office of the National Security Adviser (ONSA) to takeover all assets and liabilities of the NCWG, including all uncompleted projects;
- Its main mandate is to develop and implement a National Cybersecurity Policy for Nigeria

DfC – Summary of Mandate

- Implementing the National Cybersecurity Initiative (NCI);
- Drafting and/or proposing all relevant laws required to be enacted by the National Assembly for the security of computer systems and networks in Nigeria pursuant to our national strategies on cybersecurity;
- Establishing a National Computer Emergency Readiness and Response Mechanism with Early Warning System (EWS) and Alerts for all cyber related emergencies in the country;
- Establishing a National Computer Forensics Laboratory and coordinating the training and utilization of the facility by all law enforcement, security and intelligence agencies;
- Creating requisite technical capacity across law enforcement, security and intelligence agencies on cybercrime and cybersecurity;

DfC – Summary of Mandate.2

- Developing effective framework and interfaces for inter-agency collaboration on cybercrime and cybersecurity;
- Establishing appropriate platforms for public private partnership (PPP) on cybersecurity;
- Coordinating Nigeria's involvement in international cybersecurity cooperations to ensure the integration of our country into the global frameworks on cybersecurity;
- Executing such other functions and responsibilities as it shall consider necessary for the general purpose of promoting cybersecurity in Nigeria and fostering a framework for critical information infrastructure protection in the country.

Keep in Mind

- A good national measure should target:
- 1. Policy;
- 2. Law;
- 3. Capacity Building;
- 4. Public Enlightenment;
- 5. Public Private Partnership and Industry Alliance;
- 6. International Cooperation

Law

- Draft Bill entitled "Computer Security and Critical Information Infrastructure Bill"
- Pending before the National Assembly;
- Key mandate of the NCWG;
- Under direct supervision of the Attorney General of the Federation (AGF);
- Drafting Team comprising Legal, Technical and Policy experts;

- Process:
- A. Draft
- B. Review
- C. Revise
- D. Approve (AGF, President, FEC)
- E. Dispatch (executive bill);
- F. Public Hearing, Final Revision, Enactment

Law.2

- What the Draft Legislation is proposing:
- A. Substantive Provisions;
- B. Procedural Provisions;
- C. Enforcement Responsibility – all existing law enforcement agencies on the basis of statutory authority;
- D. Prosecutorial Authority;
- E. International Law Enforcement Cooperation

Law.3

- **Goal of the proposed legal framework:**
- **To secure computer systems and networks in Nigeria and protect critical information infrastructure in the country;**

- **In summary, Legislation seeks to criminalize 3 kinds of conducts:**
- **Conducts against ICT systems;**
- **Conducts utilizing ICT systems to carry out unlawful activities or commit crimes; and**
- **Unlawful conducts committed against critical information infrastructures (CIIP) –** deliberately targeting ICT infrastructures that affects the economic well-being of Nigeria and our collective security as a country; eg telecoms, power, oil and gas, civil aviation, etc – level of punishment much higher

Law.4
Part I – Offences & Enforcement

- Enforcement of the Act by Law Enforcement Agencies
- Unlawful access to a computer
- Unauthorized disclosure of access code
- Fraudulent electronic mail messages
- Data forgery
- Computer fraud
- System interference
- Misuse of devices
- Denial of service
- Identity theft and impersonation
- Records retention and data protection
- Unlawful Interception
- Failure of service provider to perform certain duties
- Cybersquatting
- Cyber-terrorism
- Violation of intellectual property rights with the use of a computer, etc
- Using any computer for unlawful sexual purposes etc
- Attempt, conspiracy and abetment

Law.5
Part II - CIIP

- **SECURITY AND PROTECTION OF CRITICAL INFORMATION INFRASTRUCTURE**
- Critical information infrastructure, etc.
- Audit and inspection of critical information infrastructure.
- Offences against critical information infrastructure.
- Civil liability

Law.6
Part III – General Provisions

- Jurisdiction, etc.
- Powers of search and arrest.
- Obstruction.
- Admissibility and evidentiary weight of electronic documents
- Tampering with computer evidence.
- Prosecution.
- Forfeiture of assets, etc.
- Compounding of offence.
- Order for payment of compensation, etc.
- Conviction for alternate offence.
- Power to make Regulations
- Interpretation
- Short title

Capacity Building & Awareness

- Institutional Capacity Building:
- A. Enforcement – Police Cybercrime Unit;
- B. Prosecution – Computer Crime Prosecution Unit (CCPU) for the Office of the Attorney General – recently approved by Mr. President;
- C. Judiciary – Digital Evidence Management System and Judicial Reform Project, focusing on new Court Rules and Training of officials for Electronic Evidence Handling
- D. Public Private Collaboration (PPP) - CERT – National Capability for computer emergency responses and incident handling – issues: One size fit all (joint)?, or separate for industry and Government;

- Awareness Programs: 3 pronged approach: institutional, sectoral and general public enlightenment

Global Cooperation

- International Law Enforcement Cooperation – provide adequate capacity (technical facilities and human skill) to enable cross-border information exchanges and joint LEA operations (MLAT no longer serves the purpose in view of speed and potential for multiple "forum shopping" by cybercriminals before hitting target.
- G8 24/7 Network; Council of Europe's Convention on Cybercrime; European initiative, open to all countries, currently 40 countries, including USA, Canada, South Africa and Japan. Nigeria is not a signatory member, but represented in the 24/7 Network by the EFCC;
- Our memo to Mr. President recommending Nigeria's accession to the Cybercrime Treaty

Conclusion

While no two countries or legal jurisdictions are the same, issues of cybersecurity seem to cut across many countries and jurisdictions. So, basic frameworks that focus on changes in Policy; Laws; Capacity Building; Private Industry Partnership; International Cooperation and Public Enlightenment, at the very least, should be developed at national levels, employing models adopted successfully in other countries.

If this conference makes any country here to take a look at its existing legal framework or the operational activities of her law enforcement organizations, for the purpose reforming either or both to meet the challenges of ICT, then this would be a very successful conference indeed.

THANK YOU

CONTACT

Directorate for Cybersecurity (DfC)

Office of the National Security Adviser

Three Arms Zone

Aso Rock Villa

Abuja

Tel +234-9-630-3553 to 57; Ext. 2228

Mobile +234-803-306-6004

b.udotai@cybercrime.gov.ng