
Framework for Cybersecurity in Nigeria

Basil Udotai, Esq.,

Director,

Directorate for Cybersecurity (DfC),
Office of the National Security Adviser, Nigeria

INET Africa Day

Rockview Hotel, Abuja

May 4, 2007

Quick Comments

- Unwanted Traffic: technical solutions would not work in isolation, however effective
- A combination of Technology and Law are usually required; USA CAN-SPAM Act, for instance
- Most of the unwanted traffic and other known nuisances are yet to constitute criminal conducts in most jurisdictions;
- A successful strategy must take into account disparate national legal systems, which is the most challenging whenever criminal conducts are involved; even in the offline world - MLATs
- Is pooling sovereignties a solution? CoE Cybercrime Convention, for instance
- Localization doesn't necessarily make the task any easier: is a crime committed? Who is involved? ANONIMITY is a debilitating factor, especially in Nigeria

Problems with Security

- It's a negative deliverable: you don't know when you have it, you only discover after you've lost it – *Jeffrey Schiller, Network Manager MIT Information System*;
 - Security of firm's networks is directly proportionate to the transactional and operational risks that the firm can confidently take on its network;
 - The dilemma of security: the need for simultaneous **Protection** and **Access**; Right access to the Right persons/entity;
 - Trusted Threat: employee (current and former); 3rd Party (outsourced operations); Technical Support;
 - Compounded by Mobility (wireless networks and 24/7 availability);
 - Need for Information (Data) Sharing across several platforms – Digital Rights Management (DRM) for movies and related value added;
 - Cost – security adds more cost to design and production costs; and in terms of operations is usually seen as risks whose cost easily outweigh its value;
 - Many firms feel confident that their FIREWALLS have taken care of all their security problems; **Firewall – Harrison Ford (Warner Bros)**
-

Cybersecurity – why we are worried

- Intelligent System and Networks are increasingly being employed to run mission critical services and sensitive processes in a number of sectors that are vital to our national economy – **Telecoms, Energy, Financial Services**
- Given the nexus between these vital sectors and our national economy, they constitute critical sectors to our national economic and security interests
- Thus, computer systems and networks running those sectors constitute critical information infrastructure – because their impairment would have a direct and expansive negative impact on our overall economy and wellbeing;
- Global Practice dictates adoption of two basic strategies in this regard:
 - 1. Regime for computer systems and networks security; and
 - 2. Regime for Critical Information Infrastructure Protection.
- (1) and (2) above is what is largely referred to as **CYBERSECURITY**

Security and Cybercrime

- Typically the tenets of security are:
- Confidentiality; Integrity; Availability (Survivability); Authentication; **Non-repudiation;**
- Cybercrime, to the extent that it seeks to punish – through the legal process, acts that violate the foregoing (constituents of security), thus constitutes a strategy for security or cybersecurity;
- Cybercrime is legally a technical term with two requirements under Nigeria's legal system:
 - 1. Conduct Prohibition
 - 2. Legal Consequences
- No one shall be convicted for acts in Nigeria except such act is prohibited in a written law in which a punishment is prescribed – Constitution of the Federal Republic of Nigeria
- Implication – technology alone cannot secure computer systems or networks, let alone protect critical information infrastructure – actual laws, drafted for the purpose must be enacted and enforced

System Security or Cybersecurity

- Security: Confidentiality; Integrity; Availability (Survivability); Authentication; Non-repudiation;
- Security **plus** Critical Information Infrastructure Protection = Cybersecurity
- Cybersecurity is “the prevention of damage to, the protection of, and the restoration of computers, electronic communication systems ... to ensure its availability, integrity, authentication, confidentiality, and non-repudiation” 18 U.S.C. 1030;
- Most national cybersecurity models, like our National Cybersecurity Initiative (NCI), highlight the necessity to **secure** computer systems and networks and **protect** critical information infrastructure

Concept of CIIP

- The concept of critical information infrastructure protection emphasizes the adoption of a policy aimed at:
 - 1. Identifying CIIP in any economy; and
 - 2. Creating a special compliance regime for CIIP
- Usually, this is a differential treatment for information system infrastructure (computer systems and networks) utilized on a daily basis in sectors that are **vital** to the national economic and security interests of a country;
- CIIP are defined as those systems and networks whose impairment would have a general, usually negative, effect on the National Economy and the wellbeing of the citizenry

Typical Measures

- 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
- 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

- 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 - 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 - Mandate

- 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.

Cybersecurity Framework

- Ideally national measures should touch on:
 - 1. Law;
 - 2. Capacity Building;
 - 3. Public Enlightenment;
 - 4. Public Private Partnership and Industry Alliance;
 - 5. International Cooperation

Law

- Draft Bill entitled “Computer Security and Critical Information Infrastructure Bill”
- Pending before the National Assembly, may not pass under this administration;
- 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 Law;
 - B. Procedural Law;
 - 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** – 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

Undoubtedly, the liberalization of telecoms and Internet penetration policies of government have yielded unprecedented growth in ICT, leading to increased dependence on technology for the delivery of basic as well as critical services in Nigeria amongst citizens, businesses and governments.

A cybersecurity program is therefore inescapable to compliment these great strides by Government, secure and protect the underlying ICT infrastructures and boost consumer confidence.

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

GSM +234-803-306-6004

b.udotai@cybercrime.gov.ng