

---

# **The Nigerian Cybersecurity Project: Initiative to Secure the Internet for Economic Development & Growth**

---

**Basil Udotai, Esq.**

Coordinator,

Nigerian Cybercrime Working Group (NCWG)

**AFRINET 2005**

Sheraton Hotels & Towers, Abuja

February 22 – 24, 2005

---

# eReadiness – what does it mean?

- **e-Ready** (ICT as an enabler)–
  - "E-readiness" is a measure of the extent to which a country's business environment is conducive to Internet-based commercial opportunities. Many factors are considered but the most important are: National Standards, Regulations and enforceable Computer Security and Protection Acts
  - It is also a measure of a country's ability to harness the Internet, by upgrading its commercial infrastructure and dismantling barriers to global e-commerce – **Charles Emeruwa, Consultant, NCWG**
  - Are we just surfing the net for fun, while others are turning it into a money making platform?
-

---

# What the UN is saying

- The number of Internet Users in the World reached 591 million in 2002 with an annual growth rate of 20% . No country despite their level of readiness has a negative growth rate.
  - Estimated on-line retail sales-Business-to-Customers (B2C) for 2002 were \$73 billion for the USA, \$28.29 billion for the EU,\$15 billion for the Asia-Pacific Regions, 2.3 billion for Latin America and as little as 4 Million for Africa.
  - ( stats from UNCTAD/SDTE/ECB/2003/1)
-

---

# More UN eBusiness Statistics ...

- Business-to-Business (B2B) e-commerce – 2001 annual on-line sales USA \$995 billion (93.3% of all US e-Commerce), EU ca.\$200 billion, Asia-Pacific est.\$300 billion by 2004, Latin-America est. \$12.5 by 2003 and Africa est.\$0.9 billion by 2003 with South Africa accounting for 80 to 85 per cent stats. UNCTAD/SDTE/ECB/2003/1
  - One of the most important factors hindering developing countries from achieving maximum economic potential from ICT, includes the absence of adequate legal and regulatory frameworks.....  
(United Nations Conference on Trade and Development 2003)
-

---

# What else did we find?

- **The Economist Intelligence Unit/Pyramid Research e-readiness rankings E-readiness Ranking (of 60) Country E-readiness score (of 10)**
  - **E-business leaders** 1 US 8.73 2 Australia 8.29 3 UK 8.10 4 Canada 8.09 5 Norway 8.07 6 Sweden 7.98 7 Singapore 7.87 8 Finland 7.83 9 Denmark 7.70 10 Netherlands 7.69 11 Switzerland 7.67 12 Germany 7.51 13 Hong Kong 7.45
  - **E-business contenders** 14 Ireland 7.28 15 France 7.26 16 (tie) Austria 7.22 16 (tie) Taiwan 7.22 18 Japan 7.18 19 Belgium 7.10 20 New Zealand 7.00 21 South Korea 6.97 22 Italy 6.74 23 Israel 6.71 24 Spain 6.43 25 Portugal 6.21
-

---

# Total Coincidence?

- **E-business followers** 26 Greece 5.85 27 Czech Republic 5.71 28 Hungary 5.49 29 Chile 5.28 30 Poland 5.05 31 Argentina 5.01 32 Slovakia 4.88 33 Malaysia 4.83 34 Mexico 4.78 35 South Africa 4.74 36 Brazil 4.64 37 Turkey 4.51 38 Colombia 4.24 39 Philippines 3.98 40 (tie) Egypt 3.88 40 (tie) Peru 3.88 42 Russia 3.84 43 Sri Lanka 3.82 44 Saudi Arabia 3.80 45 India 3.79 46 Thailand 3.75 47 Venezuela 3.62
  - **E-business laggards** 48 Bulgaria 3.38 49 China 3.36 50 (tie) Ecuador 3.30 50 (tie) Iran 3.30 52 (tie) Romania 3.20 52 (tie) Ukraine 3.20 54 (tie) Algeria 3.16 54 (tie) Indonesia 3.16 **56 Nigeria 2.91** 57 Kazakhstan 2.76 58 Vietnam 2.76 59 Azerbaijan 2.72 60 Pakistan 2.66
-

---

# What we have determined

- Digital Divide
  - Cyber Security
  - Digital Opportunities
-

---

# What Law?

- What law?

It is NOT a crime in Nigeria except conduct is prohibited in a written law in which a punishment is also prescribed

- Conduct Prohibition Requirements - CFRN;

Even where conduct amounts to a crime in Nigeria, the acts criminalized may not be punished except through a judicial process exists where evidential rules enable trial and conviction of offender

- Legal Consequences Requirements.

---

---

# Why Legal Security & Protection?

- Technology does not provide absolute security or protection; even where security is absolutely sufficient, law is required for attempts
  - Law to bridge the gap: Technology + Liability = PROSECUTION
  - International Law Enforcement Assistance = “Dual Criminality Requirements” – I LOVE YOU virus; led to Cybercrime laws in the Philippines,
  - Official institutional authority to enforce law, handle CERT (UK Air Control System 2hr downtime, UKHTCC to the rescue!) and execute bilateral (MLATs) and multilateral treaties (CoE Cybercrime Convention)
-

---

# Why now?

- eReadiness Ranking - Do we need more excuse?
  - Constitutional prerogative of government to enforce law: sophistication of crime or high-tech nature of media not excuse for inaction;
  - Success in ICT in Nigeria = Fastest growing telecoms market in Africa – ITU, more than \$4 billion FDI in 3 yrs (NCC);
  - Increasing dependent on ICT: personal, business and government;
  - Telecoms infrastructure critical to Nigeria's economic and social well being;
  - Damage will have very expansive effects, with grave social, economic and political consequences;
  - Telecoms is a “test case” for other FDI
-

---

# Global Trends

## What are other countries doing?

- Enacting legislation – substantive and procedural laws that criminalize certain activities online and create procedures for investigation, prosecution, punishment and sentencing of offenders, while enhancing global collaboration in cybercrime and cybersecurity enforcements
  - US, UK, and SA – laws affecting Computer Misuse, Computer Privacy, Electronic Transactions, Computer Crimes, Computer Security Enhancement, Data Retention Laws, Digital Signatures and Computer Evidence Laws
  - Internationally: G8 24/7 Network; CoE Convention on Cybercrime – now Treaty open to non – European signatories – USA, Japan, South Africa, etc have signed – model, generally acceptable worldwide; OECD, WTO, UNCTAD, UNCITRAL, etc
-

---

# **The Nigerian Cybercrime Project**

## **What is this about?**

- Two things:
  - Security of Computer Systems and Networks;  
and
  - Protection of Critical ICT infrastructure in  
Nigeria
-

---

# The Nigerian Cybercrime Project

## Background

- Presidential Committee on Cybercrime
  - Report recommended creation of a legal and institutional framework for cybercrime in Nigeria
  - Create a central agency to enforce cybercrime or situate responsibility within existing law enforcement institution
  - Create the Nigerian Cybercrime Working Group (NCWG) as an inter-agency body of law enforcement, intelligence, security and ICT institutions, plus private sector
  - Proposed a Draft Nigerian Computer Security and Protection Act
-

# **The Nigerian Cybercrime Working Group (NCWG)**

- **an Inter-Agency body made up of all key law enforcement, security, intelligence and ICT Agencies of government, plus major private organizations in the ICT sector; including 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 Chairman and one Coordinator.**
- **ToR include public enlightenment – CYBERSECURITY FORUM for the Financial Services Sector, building institutional consensus amongst existing Agencies, providing technical assistance to the National Assembly on Cybercrime and the Draft act; laying the groundwork for establishment of institutional capacity in Nigeria, etc.**
- **Commencement of Global cybercrime enforcement relations – CCIPS (USA), NHTCC (UK), NPA (SA)**

---

# **Draft Nigerian Computer Security and Protection Act**

- **Substantive – criminalize conducts against ICT systems, using ICT systems and targeting critical ICT infrastructures**
  - **Procedure – judicial procedures for investigation and prosecution**
  - **Including data retention obligations on all ISPs, TSPs, ASPs [for a period of 5 years]**
  - **Constructively amend all traditional Intellectual Property laws and the Evidence Act: not just legal enforceability, but also prohibiting the production and distribution of devices manufactured specifically to circumvent security measures for protecting software against copying**
  - **Establish institutional framework for enforcement in Nigeria**
  - **Creating global law enforcement cooperation with international law enforcement organizations Worldwide**
-

---

# Conclusions

Prevent, Protect and Prosecute - 3Ps

With technology you can **prevent** and **protect** your system, but you need to also be able to investigate and **prosecute** offenders who utilize ICT systems for illegal purposes!

---

---

# THANK YOU

CONTACT:

**Nigerian Cybercrime Working Group (NCWG)**

**Office of the National Security Adviser**

**Three Arms Zone**

**Aso Rock Villa**

**Abuja**

**09 222 3000;**

**GSM 0803 306 6004**

**[b.udotai@cybercrime.gov.ng](mailto:b.udotai@cybercrime.gov.ng)**

**[www.cybercrime.gov.ng](http://www.cybercrime.gov.ng)**

---