Strategy for Addressing National e-Governance Risk

Abstract:
The advent of e-governance has ushered in a new digital innovation in the electronic delivery of public services and information between the government and the citizens. However, the tremendous capabilities of e-governance is threaten due to the risk factors inherent in the current e-governance system .

Unfortunately, e-governance risk assessment from cybersecurity point of view receives little or no attention in the handlers of e-governance projects in the country. Cybersecurity of critical components of e-governance infrastructure is currently becoming an extremely urgent subject matter worldwide. Thus, this paper seek to highlight the cybersecurity risk and structural weakness of e-governance, the root cause and the impact on the overall direction e-governance, as well as provoking strategic needs for structural re-adjustment through fundamental engagement of the framework of cybersecurity strategy.

The E-Governance (e-G)

E-G is the deployment of internet and the World Wide Web for delivery of government information, and services to the citizens (United Nation 2006; AOEMA, 2005).

The World Bank defines e-government as "the use of information and communications technologies by governments to enhance the range and quality of information and services provided to citizens, businesses, civil society organizations, and other government agencies in an efficient, cost-effective and convenient manner, making government processes more transparent and accountable and strengthening democracy."

This involves engagement of information technology, communication technology and other web-based telecommunication technologies that have tremendous capabilities to deliver public services, information and data to citizens, while enabling proactive citizens' participation and active engagement in governance, consultation, deliberation, transaction, services delivery, and knowledge policy.

Therefore e-G uses ICT to facilitate and improve on the efficiency and effectiveness of service delivery in the public sector. (Jeong 2007).

The e-G demonstrate applications of ICT to facilitate the operation and the disbursement of government information and service delivery. It therefore, rely heavily on the internetwork of ICT infrastructures, internet and non-internet applications to aid the operations of government.

The e-G system has gone beyond this level to embrace convergence capabilities of ICT, computers, internet, telecommunications, multimedia, digital broadcasting as demonstrated in the recently deployed unified communications technologies in government to government real live communication.

2Main Category of e-G

- **Online government;** Internet/Virtual Private Network /Intranet based governance
- **Non-Internet (Offline)/*Smart* governance? Yes!:** It involves non-internet framework which include SMS, MMS, Wireless networks, bluetooth, biometric identification, e-voting, PDA, etc.

Operational Scope of e-G

- Traditionally, e-G is centered around the operations of government
- Currently, e-G now include citizen engagement and participation in governance through the use of ICT to achieve better governance.

The Component of e-G

The e-G is digital interactions which consists of following components

- Governance
- Information and Communication Technology
- **Business process re-engineering i.e the nature of the** service delivery system- cyberspace!
- e-citizen at all levels of government i.e Federal, state, local government and international.

Mode of e-G delivery & their Limitations

i. Government to Citizens (G2C)
Uses CRM principles, where citizen is seen as customers or consumer. E.g Nigerian Immigration Portal

ii. Government to Business (G2B)
Government transaction dealing with contractors/organize private sectors. E.g Nigeria Stock Exchange Portal, CBN portals, e-payment system

iii. Government to Employees (G2E)
E.g Nigeria Pension Scheme System,

iv. Government to Government (G2G)
e.g Unified Communication via a structure dedicated Virtual Private Network. Usually among heads of state,

Strategic Importance of e-G

I. Facilitate faster disseminations of government information
II. Allow users to engage in real life feedback dialogue
III. Simply government transaction process
IV. Transform citizen into an active participant in governance
V. Reduce cost of governance via elimination of physical barrier
VI. Simplify the process of governance

Outcome of E-Governance

1. **From Government Perspective**
The outcome of e-governance is to **transform** the entire relationship between the public sector and users of public sector through a creative utilization of Electronic delivery system, in a way that strengthen a nation and grow the economy immeasurably in more transparent, cost effective and premeditated way. **How far have we been able to achieve this outcome?**

Basis of Evaluation: According to United Nation Public Administration Network's Global e-Governance Readiness Index- Where is Nigeria's position?
The United Nations Public Administration Network conducts a bi-annual e-G survey 191 member states including Nigeria based on two main indicators;

- State of e-government readiness based website assessment, telecommunication infrastructure and human development
- and Extent of e-participation.

The Verdict: No African country listed among the top 50 countries – UN's 2010 e-Government Readiness Index

2. **From Cybersecurity Perspective**
   To achieve a **trusted e-services** built and driven on the core principles **Confidentiality, Integrity** and **Availability (CIA)** in a way that focus on the Effectiveness, Efficiency, Flexibility & Transparency which are the overall goals of information security.
   How far have we been able to achieve this outcome? Basis of Evaluation? Not available!

   - Confidentiality i.e protecting sensitive information from unauthorized disclosure or intelligible interception, eavesdropping.
   - Integrity: Preserving the accuracy and completeness of information and software; protecting data from unauthorized, unanticipated or unintentional modification
   - Availability: Ensuring that information and vital infrastructural services are available when required

Critical Success Factors in Trusted E-Governance Delivery Strategy

To achieve a **trusted e-services**, e-Governance strategy needs to focus on the central principles of Cybersecurity's CIA.

How? .

- The design, development, deployment and maintenance of eGovernance facilities and applications must be built on a sound fundamental framework of Information security.
- Provision of coordinated roadmap, standards, procedures, and central regulatory information security regime for the public sector in Nigeria.
- E-Governance *information*, *data*, *resources* and *infrastructures* must be declare **critical nation assets** that must be secured at all levels covering applications, Infrastructures and operation and Management.
- The provision of trusted e-services should be confidential, and in no way violate the privacy of either the government or the citizens, which would comply with the existing international standards, requirements and relevant legal and statutory policies.
- The citizens must know the information about the available e-services; must be aware of the benefits of these e-services, should be able to locate the e-services easily;
- The e-services must be accessible to all members of the intended target citizens
- The information from the e-G services should be comprehensive, correct, readily available, and easy to understand with readiness to bear the burden of the responsibilities and the consequences of operations .

To protect and secure the "value" of information in e-G, effective information security measures that will limit the e-G risk exposure need to be integrated at the foundation level of e-G design and development, and implemented harmoniously throughout the operational cycle.

The E-G Security Risk

The nature of development and deployment of e-governance in the country, which is based on internet or intranet hosted via Virtual Private Network, has a fatal security risk due to the underestimation of the complexity of threat and vulnerability of e-G network.

The E-Governance in Nigeria has a high level of threat potentials with high level vulnerability rate. i.e Nigeria has a very high risk factor.

Generally speaking, the security risks e-government facing includes the following aspects:

What is e-G Threat?
From Information security perspective, threat is any activity that can cause possible danger to the resources, information, data, and operation of e-G system in a manner that would affect the confidentiality, integrity or availability of e-services delivery or system.

E-Governance Risk Exposure			
Types of E-G Threat	**Nature Threat**	**Ultimate Goal**	**Mitigation Strategy**
High Risk Threats	• Well-resourced, highly-motivated groups of cyber-warriors who are both aggressive and pervasive. • Numerous attack vectors including email, social media, and apparent trust paths like those with contractor facilities • Use of zero-day attacks and exploitation of weak credentials are common • Often referred to as the Advanced Persistent Threat in public media • Can be internal or externally perpetuated • Infrastructural/natural disasters either by the nature or man made	Attack of national Economy /security Political propaganda Industry espionages Intellectual property Backdoor Activitism (E.g wikileak)	**National Cybersecurity Readiness & Response Strategy Covering the following 5 measures** ♦ **Technical** ♦ **Local Expertise** ♦ **National Structures** ♦ **Legal** ♦ **High-net worth awareness**
Medium Risk Threats	• Criminals targeting identity and money • Varying levels of technical sophistication • Botnets and Bot Herders • Usually externally perpetuated	Target individuals or entities, usually for criminal purposes like stealing someone's identity and ultimately their money Target agnostic	**Strong enforcement of industry best**

		towards Federal government or private company Individuals and groups of varying technical	**practices will help significantly with stopping both Low and Medium Risk Threats**
Low Risk Threats	• Standard Internet Pollution/intruders/irritants • Threats against every user • Unsophisticated but tactical • Technical in nature – worms, viruses, script kiddie hackers • Can be internal or externally perpetuated	Nuisance variety - do not target specific individuals or entities for any specific purpose	

What is e-G Vulnerability?

From Information security perspective, this is a structural weakness cause by critical flaws or errors of technical oversight usually during the design , development, implementation or configuration of e-G system which could be externally or internally exploited by a threat.

Please note:

- Risk exposure is determined where there are existence of threats and vulnerability.
- In e-G, system vulnerabilities are the main doors through which threat can manifest.
- **The major worries of Information Security is not the threat to the e-G, but the massive vulnerabilities of e-G structural component, e.g software flaws, inferior substandard ICT hardware, poor configurations of mission critical system, unregulated policies, etc.**
- **E-G vulnerability are usually hidden and undiscovered**
- **Most unfortunately attacker or criminal are usually smarter than e-G planners. Why? Because they discovered vulnerability faster and long before the e-G planners discover them**

Why Are We Concerned About Cyber Security?

Our Country cyber landscape is electronically porous, structurally uncoordinated, unprepared and exposed! **On the internet, either online or offline, we are like a structurally exposed glass house with weaken frameworks, and porous windows and doors, with gullible occupants operating within a highly vulnerable environment.**

Absence of sustained commitments across all the government agencies. Hardware, software, security are weakly integrated into the system life cycle.

Strategy to address e-governance risk

- National e-Governance system deployment requires strong IT governance
  - Integrating core principles of information security into National e-G framework
- National Cybersecurity Strategy via 5-framework approach; Technical

- Instances of Cybersecurity measures that address E-G Risk
  IOC Case study: National Capacity Building – IOC
  PKI case study: securing National e-governance communication
  Honeypot case study: Building e-security counter measure against external threat.
- Compliance Case study: Industry ISO Standards Vs Govt Regulation