Response Provided By

**Nigeria Internet Governance Forum (NIGF)**

Questions:

* **What are the typical roles and responsibilities of your/each of the stakeholder groups in making the internet a secure and safe place for people to socialize and conduct business?**

1. The Nigerian Internet Governance Forum (NIGF) and ICT & Cybersecurity stakeholders’ forum provide local awareness for policy makers on cybersecurity and public Internet safety. We collaborate with heads of government agencies relevant to ICT development, Telecommunication regulation and captains of industry in the ICT industry to dialogue on how to build trust and entrench Internet user confidence on the use Internet as a tool and a platform for business and economic development.
2. We engage the public on cybersecurity awareness through consistent participation in Nigeria Internet Governance and similar event such as e-Nigeria Summit, National Television Programs where we ensure regular discussion on a secure cyberspace, share emerging issues on Internet safety as well as provide relevant capacity building on Personal & Corporate Internet Safety Responsibility (PCISR).
3. We engage the use of social media apps most especially WhatsApps to create discussion forum where instant Internet security incidences and mitigation reports are distributed and shared among individual members of the forum on real live and upwardly mobile basis. This approach has helped escalate incidences of internet safety issues and provide community awareness.
4. We engage in local high level political discussions with senior public officers and political offices holders within the executive and legislative arms of the government on possible policy and legislative intervention on cybersecurity.
5. The group collaborates with key industry players and industry regulator on the development of technical code of conduct and accountability for the ISP and operators in the Internet Industry ecsystem.
6. The local media often takes on internet safety and hygiene topics to the centre stage of public readership and internet users

* **What are some of the typical communication mechanisms between stakeholder groups to discuss cyber security related concerns?**

1. We instituted ‘’Stakeholders Forum on Cybersecurity’’ to foster communication on policy issues, cooperation, and understanding of common emerging Internet security incidences among local stakeholders.
2. We created social media forum using Whatapps for continue dialogue and sharing of contentious Internet safety policies issues. The Whatapps forum enables direct communication among the share group.
3. NIGF has as its main dialog sub-theme, **Trust and Cybersecurity** every year, this subtheme attracts the highest interest of the stakeholders as each community, law enforcement, government, civil society, academia, private sector and technical community come together to dialogue on how best to make internet safer for the users, including children and young people

* **How can cybersecurity cooperation and collaboration be enhanced particularly in developing and least developed countries?**

1. There should be mechanism for creating awareness among the key actors on common impact of Cybersecurity dialogue that will inspire actors to engage more in the discussions and proffer solutions.
2. Since Government is the prime business mover in Nigeria, it is very critical that Government be engaged and exposed to the need for non-governmental institutions’ participation in policy making related to cybersecurity. The users and providers of services must necessarily participate locally to form a strong platform for discussion that elicits actionable recommendations for a common impact that should emphasis on Cybersecurity Cooperation and awareness on on local security, economy, crime, and social development.
3. Local High-level Political leaders should be engaged through appropriate regular consultation with the goal of drawing their commitment to Cybersecurity policy issues relevant to local economy, crime, development program and their relevance in international community.
4. There should be capacity building for local media and press organizations on the reporting of cybersecurity related events, news and development relevant to local socio-economic and political activities most especially intersecting reporting with their evolving issues on human rights abuses, spread of violence, internal conflict and crime, as well as risk exposure of their emerging economy and nascent democracy within global digital ecosystem.
5. A multi-stakeholders consultative forum should be developed bringing the Government, private sector, and civil society together on common dialogue on cooperation and collaboration.
6. For instance, in Nigeria, the Nigerian Internet Governance Forum (NIGF) has consistently pushed for strong dialogue and cooperation on Cybersecurity since its inception, leveraging on the multi-stakeholder nature of the forum. The output of the discussion has always been brought directly to the attention of the policy makers, who themselves participated in the forum.

* **What are some notable existing best practices and examples of successful collaboration and cooperation amongst stakeholders and specific actors that have helped improve cybersecurity?**

1. There exists in Nigeria an **Interagency network for collaboration** that has worked well for the country in producing the Cybercrime Act 2015. It involves policy synergy, cooperation, and collaboration among all government agencies thus evolving into a single point of contact and response on National Cybersecurity. The outcome produces a single corridor approach to engaging other non-government entities on partnership.
2. A **Cybersecurity Nigeria mechanism,** spurred a cohesive approach on principles of engaging the whole of country’s stakeholders. It provides a mechanism for building trust, engaging and uniting all stakeholders on common national cyber issues, through negotiation and understanding. This approach worked well during the development of Nigeria Cybersecurity Policy and Strategy 2013-2015. It contains 5 elements; i.e. the government via the involvement of Interagency network; coalitions of private sector groups; Service providers, coalitions of Civil Society Organizations; Coalitions of Multinationals operating in Nigeria; and International community.

* **What are some examples of best practices in ‘Cyber security Situational Awareness’ where different organizations have worked together, specifically with law enforcement agencies and other specialists?**

1. In the context of ‘’Cybersecurity Situational Awareness’’ which is hinged on collaboration and cooperation framework, *Cybersecurity Nigeria* best practices approach is developed indigenously spearheaded by the nation’s foremost coordinator of all security organizations, i.e. Office of National Security Adviser (ONSA). The ONSA mobilizes all security and para-security organizations including the Military, Police, and other law enforcement agencies, through the Interagency network framework, into Cybersecurity Nigeria forum, a local multi-stakeholders’ Consultative platform for building common consensus and trust through cooperation and collaboration on Cybersecurity Strategy. It remains the best example of multi-stakeholder intervention model led by law enforcement working closely with representative of private sector and other non-government entities.

* **What are other related or different topics that your organization would like this BPF to address moving forward, both in 2016 and beyond?**

1. The need to bridge critical knowledge gap on cybersecurity awareness and advocacy.
2. Building a framework for regional cooperation on Cybersecurity
3. Multidisciplinary nature of cybersecurity intervention
4. Global protocols for achieving Cybersecurity cooperation i.e. need for framework or best practices on Cybersecurity Diplomacy to help nations build trans-jurisdictional cooperation and partnership.
5. Child online protection and public safety online
6. Building Trust between the Civil Society and the Government in addressing global intervention on cross boarder cybercrime.
7. Cybersecurity as critical element in achieving Sustainable Development Goals .