Cybersecurity Best Practice Forum

Internet Governance Forum Mauritius (IGF Mauritius)'s input

1. **How does good Cybersecurity contribute to the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?**

   As physical security brings trust in the real world, Cybersecurity contributes to bring trust for the virtual world including the use of and the growth in ICTs and Internet Technologies.
   Good Cybersecurity is not a matter for the Government only but it encompasses all stakeholders related to ICTs.
   - The Technical Community is there to devise technologies for Cybersecurity.
   - The Government - to enact local laws, have bilateral and multilateral agreements with other countries and adopt international conventions
   - The Academia – To bring into curriculum the subject matter of Cybersecurity and to form Cybersecurity engineers
   - Civil Society – To do the work at grassroots level and sensitize the population on the dangers of cyber threats on best practice on Cybersecurity
   - Inter-Governmental Organisations – Help in bringing on Conventions, like the Budapest Convention on Cybercrime, which when Governments adopt help in combating cybercrime and safeguarding the country's Cybersecurity.

   As the use of the Information and Communications Technologies (ICTs) and the Internet Technologies help in the attainment of the Sustainable Development Goals (SDGs), good Cybersecurity contribute to the growth and trust in ICTs and Internet Technologies and subsequently help in the support to the Sustainable Development Goals (SDGs)

2. **How does poor Cybersecurity hinder the growth of and trust in ICTs and Internet Technologies, and their ability to support the Sustainable Development Goals (SDGs)?**

   Poor Cybersecurity hinders the growth of ICTs and Internet Technologies as it brings distrust.
   People will not have faith in the ICTs and Internet Technologies if they are victims of cyber criminality. This is not because of the use of ICTs and Internet Technologies but because they are not adequately protected due to poor Cybersecurity. When this happens, people will not use the ICTs and Internet Technologies, which is useful in the attainment of the Sustainable Development Goals (SDGs). In short poor Cybersecurity has an impact on the use of ICTs and Internet Technologies and ultimately on the attainment of the Sustainable Development Goals (SDGs)

3. **Assessment of the CENB Phase II policy recommendations identified a few clear threats. Some policy options to help address, with particular attention to the multistakeholder environment, the following cybersecurity challenges:**

- Denial of Service attacks and other cybersecurity issues that impact the reliability and access to Internet services – Development by the Technical Community technologies to counteract DDos Attacks and international conventions to punish cybercriminals
- Security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfill critical goals such as payments – R&D by the Technical Community on Security Software and Mass Sensitization by the Civil Society on best practice and optimal use of apps and other mobile software
- Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended – Sanctions by the International Community to Governments making an abusive use of the effects of technologies. Intergovernmental Organisations have an important role to play
- Confidentiality and availability of sensitive information, in particular in medical and health services – Civil Society as a watch-dog to ensure that no sensitive and confidential information is disclosed
- Online abuse and gender-based violence – Enactment by Governments laws that will punish these types of cybercrime.
- Security risks of shared critical services that support Internet access, such as the Domain Name System (DNS), and Internet Exchange Point (IXP) communities – Implementation of DNSSEC and other technologies. Technical Community with the help of other stakeholders.
- Vulnerabilities in the technologies supporting industrial control systems – To be addressed urgently by the Technical Community
- Use of information collected for a particular purpose, being repurposed for other, inappropriate purposes. For instance, theft of information from smart meters, smart grids and Internet of Things devices for competitive reasons, or the de-anonymization of improperly anonymized citizen data. Enactment of appropriate laws and amendments by Governments to criminalize such activities.
- The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis. Technical Community has to be in pace to cater for such processes.
- Unauthorized access to devices that take an increasing role in people's daily lives. - Criminalize such access by enacting appropriate laws by Governments.
- Other: describe a Cybersecurity issue critical to developing the SDGs in ways not listed above relevant to your stakeholder community -

Virus, malware and other Ramsomware attacks to be severely criminalized by all Governments and the Civil Society has an important role to play to sensitize users of the best practice for computer safety and protection against all these threats.

4. **Many Internet developments do not happen in a highly coordinated way - a technology may be developed in the technical community or private sector, and used by other communities and interact in unexpected ways. Stakeholders are managing complexity. This both shows the strength and opportunities of ICTs and Internet Technologies, but also the potential risks. New technologies may be insufficiently secure, resulting in harms when they are deployed: conversely, we may adopt security requirements or measures that prevent the development, deployment, or widespread use of technologies that would generate unforeseen benefits. Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?**

   The responsibility of the Private Sector is to ensure that technologies are developed not only taking the cost factor in mind but also the security aspect of it. The technical community should hear a lot from the Non-Governmental Organisations and other stakeholders before designing technology. Perhaps the IETF should broaden its membership to include all stakeholders not only the techies. The International 0rganisations should ensure that all Governments do adopt conventions and agreements. The Governments should ensure that they are up to date with their laws to ensure safeguard of critical infrastructure and punish cybercriminals and the Academia should be ready to bring into curriculum technologies recently developed or adopted. If each of the individual stakeholders assumes their responsibilities correctly we are sure that Cybersecurity won't hinder the further development of the ICTs and Internet Technologies.

5. **What is for you the most critical Cybersecurity issue that needs solving and would benefit most from a multi-stakeholder approach within this BPF? Should any stakeholders be specifically invited in order for this issue to be addressed?**

   The recent Ramsomware attacks have shown how vulnerable we are when we are using a common operation System. We think that this issue needs to be tackled urgently and bring on the table all parties, the Private Sector (The OS provider), the Technical Community (to provide alternatives), the Government (to update laws and regulations), the InterGovernmental Organisations (to come to a coordinated approach by all Governments), the Academia (to update on curriculum on new technologies) and the Non-Governmental Organisations to sensitize users on the dangers of not being adequately protected and the measures to take to make a Cybersecurity as reality.