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 with any new phenomenon, the adaptability of any product and service is hugely affected by Trust. ICT and related internet technologies is not an exception. With more and more economic and social transactions moving to the online world, users do not have much of a choice but to adopt to these spectacles. ICT's and associated applications are known to have the supported the SDG's by reducing the transaction cost, increasing transparency and speed on knowledge and information transfer. However, the sustainability depends profoundly on how well the security of the platform (read ICT and Internet) is being maintained.

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)?

As in case of physical world trust is build and maintained when what is being promised is being delivered, that too with an acceptable quality. While the intended security may not directly affect the functionality of the service delivered but significantly affect the quality. In absence of optimum control, it also bolsters the stakeholder confidence on the platform which is replicated across the community as a wildfire. It sometime becomes difficult to quantify the damage in reputation due to its direct association with the intangible emotion such as trust. It's a kind of permanent damage that affect the reputation and future adaptability of the technology. With the borderless and nationless reach of the technology the impact is also extravagated. With the increasing complexity of the technology development and the less and less awareness (both interrelated), the adoption is directly proportional to the amount of trust we have. Hence, it's important that this trust is build and maintained. A holistic cybersecurity approach based on the strong risk and information security principles is required to address this challenge. At a minimum, the risk must be assessed on the following three principles application to any information assets.

- Confidentiality
- Integrity
- Availability

All the mentioned phenomenon must be clearly understood and the applicability assessed by performing a risk assessment of the technology. Controls must be implemented to ensure that the risk is clearly understood and treatment applied accordingly.

3. Assessment of the CENB Phase II policy recommendations identified a few clear threats. Do you see particular policy options to help address, with particular attention to the multi-stakeholder environment, the following cybersecurity challenges:

    a. Denial of Service attacks and other cybersecurity issues that impact the reliability and access to Internet services

Accountability need to be identified and ascertained to ensure that the originating threat vector is made responsible and penalized for these attacks. May it be individual, organization or nation state.

    b. Security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfill critical goals such as payments

Manufactures and technology providers should be encouraged to device mechanism that makes the security implementation and monitoring easier. Security by design is made mandatory.

    c. Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended

Privacy and Data Governance policy/ laws need to be formulated and provide clear guidance on how these threats , if materialized by authority, need to be addressed.

    d. Confidentiality and availability of sensitive information, in particular in medical and health services

These information and services need to be made available on “need to know” basis. Availability has to be tracked and ensured that it complies the SLA, agreed with the stakeholders.

    e. Online abuse and gender-based violence

Abuse and gender based violence (online or offline) has to be addressed in line with the land of the law. Technology providers should provide means that these can be monitored and rules implemented.

    f. Security risks of shared critical services that support Internet access, such as the Domain Name System (DNS), and Internet Exchange Point (IXP) communities

Contingencies need to be built around these shared and critical resources (likes of Disaster Recovery capabilities, Dual control etc.)

    g. Vulnerabilities in the technologies supporting industrial control systems

Technology developer need to be hold responsible for the vulnerability. Patches implemented on a timely basis. Operational responsibility for the internal maintenance team has to be clearly defined as well.

h. 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

Once identified and proved the culprit must be charged in line with the governing law. The victim of the breach need to be compensated, such provisions should be included in the law

i. The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis

Accountability for the developing house should be defined and monitored.

j. Unauthorized access to devices that take an increasing role in people's daily lives

Analogy to this is burglary. It has to be treated at par and victim compensated

k. Other: describe a cybersecurity issue critical to developing the SDGs in ways not listed above relevant to your stakeholder community (100 words or less)

NA

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?

With this level of coordination and complexity, it becomes increasing important that we have a mature model of defining responsibility and accountability. Unit Testing and Integration testing must be performed consistently and the outcome documented in a comprehensive manner. There should also be a regulatory transparency in the level of information that are shared across the various stakeholders. The transparency in the information flow is an asset for the testing community to ensure that cybersecurity risks are appropriately assessed and control suggested accordingly. It becomes imperative for all the community involved that the testing protocols are followed appropriately and recommendations applied on timely basis.

5. Where do you think lies the responsibility of each stakeholder community in helping ensure cybersecurity does not hinder future Internet development?

All stakeholders within the internet development, operation, management and governance space has a responsibility to integrate cybersecurity assessment and control in their respective Standard Operating Procedures (SOP). The executive in these spaces have the responsibility to provide executive strategy and resources to ensure that these SOP's are complied with.

6. 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?

At the outset, we need to understand and acknowledge that cybersecurity of any technology and platform is an evolutionary process. All the stakeholders need to have the expectation clearly staged and cascaded within the community. To me, what is most important is that the Risk management methodology for the cybersecurity management for the Internet as to be evolved and given its due importance. It is important that we start understanding and acknowledging that there is nothing called a 100% security. The idea should be understanding the most applicable risk to the platform in the given scenario and we have the control mechanism that need to be implemented in case that identified risk materialized.

To achieve this that we have Risk management professionals involved and engaged to have this addressed by the various community.

Submitted by: Mohit Saraswat