CCAOI™

Representing the ecosystem of Internet -Bharat Model

CCAOI Submission to 2018 IGF BPF Cybersecurity

Submitted by: Amrita Choudhury
Director, CCAOI, India
amritachoudhury@ccaoi.in

Stakeholder Group: Civil Society

1. How do you define a culture of cybersecurity?

   CCAOI response: A culture of cybersecurity would be an environment where people belonging to different stakeholder communities have adequate information and knowledge regarding cybersecurity and the related threats; are equipped to take precautions by following agreed norms and values to protect not only themselves but also others from cyber threats.

2. What are typical values and norms that are important to you or your constituents?

   CCAOI response: From CCAOI's perspective any norm should provide:

   - Clarity of the potential cybersecurity risks and best practices to follow, to prevent that. The norms should be easy to understand and abide by.
   - Proper support through training to abide by the norms.
   - Awareness of the legal provisions against cyber crime.
   - Regular updation : (i) at the technical level (patches, updates, etc.) to protect oneself (ii) Information on the latest developments including best practices globally on the subject.

3. Within your field of work, do you see organizations stand up and promote specific cybersecurity norms? This can be either norms at an inter-state level, or norms that only apply within your community or sector.

   CCAOI response: In India, we have the legal provisions in the Information Technology Act (IT) to protect against cyber crime and the Indian CERT team has been working on areas of Cybersecurity.

   Further, there are organizations, industry bodies and civil societies who are promoting best practices to protect organizations, individuals online against cyber threats. Implementation and adherence of these initiatives seem to be a challenge. Additionally, each of these are working in silos. There is an urgent need for weaving in all such initiatives under one umbrella and drafting a unified set of norm, which today is missing.

The advantages of having a single norm would be that it is easier to implement and can provide more benefit across different stakeholder communities. However, it should be prepared by involving all stakeholders for a balanced thought out framework.

4. Are there examples of norms that have worked particularly well? Do you have case studies of norms that you have seen be effective at improving security?

   CCAOI Response: NA

5. Do you have examples of norms that have failed (they have not seen widespread adherence), or have had adverse effects (living up to the norm led to other issues)?

   CCAOI Response: The Implementation of norms and their adherence is a major concern. Making the process too complicated or not explaining the norms clearly and lucidly to the people who would be implementing or abiding by the norm at times have adverse effects as people take it as a burden and do not follow it wholeheartedly.

6. What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?

   CCAOI response: Firstly, there is a need for indepth research on the subject. Secondly, it is important to create an awareness among all stakeholder groups –government, business, civil society on the threats of cyber security; the importance of having common cybersecurity norms; advantages of following norms and the implications of not adhering to them.

   Training and capacity building will help to make communities aware and adopt norms. Simultaneously, IGF and the NRIs, which are open platforms, should encourage more discussions on best practices and ways to address concerns of implementing cybersecurity norms, which will be of immense benefit to the community.

7. Within your community, do you see a Digital Security Divide in which a set of users have better cyber security than others? Is this a divide between people or countries? What is the main driver of the divide?

   CCAOI response: Yes the Digital Security Divide is quite evident. The divide can be clearly seen between developed and developing nations, literacy and socio-economic levels. The digital security divide is higher in developing nations, people with lower literacy levels or coming from lower socio-economic strata. This can be attributed to the lack of training or awareness of online safety.

It is also seen within an organization depending on the level of understanding of security concerns. For example, within an organization a security professional will be more conscious of security issues, whereas a member of the sales team may not be quite conscious/aware about security issues.

Lack of education and awareness of the security threats and their impact is one of the major factors of this anomaly.

Therefore the need of the hour is to initiate more capacity building and training on different aspects of Cyber Security and encourage best practices or norms, which community can mutually adhere to reduce this digital security divide.