1. How do you define a culture of cybersecurity?

   To me a culture of cybersecurity means the attitude, mindset, belief, experience of people regarding cybersecurity. By adopting this culture, employees of any organization will consider cybersecurity as an integral part of their lives. An organization with good cybersecurity culture is tend to have a strong human firewall and less prone to cyber-attacks.

2. What are typical values and norms that are important to you or your constituents?
   Following cybersecurity standard and best practices are important to me. The technical best practices are having updated anti-virus, regular patching, mitigate the impact of attacks, remove the vulnerability etc.

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.

   Within my field of work, I see very few organizations stand up and promote specific cybersecurity norms. Cybersecurity has always been the overhead in many organizations. Business continuity has dominated so far over cybersecurity. This will continue until people understand the intensity of cyber-attacks.

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?
   So far I have noticed the norm of having effective and enforced processes and policies have worked particularly well. Many organizations are getting focused on building processes and policies. In many companies they exist but no enforcement is in place. I have seen processes and policies approved and enforced by top management has proved to be very effective at improving security.

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)?

   I have seen while trying to build a cybersecurity culture people create a culture of fear which has the adverse effects. When we highlighted the damage done by the cyber-attacks to the people it seemed people move away from it.

6. What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?
   I think the effective methods of implementing cybersecurity norms is creating awareness. People need to know why it is important to follow cybersecurity norms and what are the consequences if someone doesn't follow. The implications of not following the norms

worldwide should be well communicated by awareness session. At the same time management team should emphasize on cybersecurity as well. The enforcement has to be from the top.

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?

   Within my community I do see a set of users have better cybersecurity than others both between people and in countries. For people the main driver of the divide is people's mindset, attitude and beliefs towards cybersecurity. For countries the main driver of the divide is the susceptibility of getting attacked by other countries. Also the factor that how many times they have become the victim by cyber-attacks and the damage done by it.

Afifa Abbas
Information Security and Governance Lead Engineer
ICANN fellow (ICANN58 and ICANN60)
Dhaka, Bangladesh