BPF cyber security IGF 2018

How do you define a culture of cybersecurity?

Cyber security culture is the local values and perception of different stakeholders and how they behave including the trends and pattern of different techniques to mitigate the cyber securities issues and challenges within the internet ecosystem. It includes various adaptation and testing process within the innovation and development process of new technologies.
https://www.slideshare.net/ShreedeepRayamajhi/cyber-security-and-current-trends

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

Most of the time norm is about persuasion, and the persuasiveness of appeals to adopt various norms depends on how they are presented to potential adopters. We learn from the experience and adopt as with live event and experiences. Norms can develop in a variety of ways, particularly through habit and adaptation process. Some norms emerge spontaneously without any particular actor having any particular intent and then become entrenched through habit. In any group that interacts regularly, norms develop simply through expectations shaped by repeated behavior.

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.

Coming from a least developed country in Asia the general practice of cyber security culture is something that is just evolving. Especially, when you talk about cyber security auditing and other compliance the overall concept is just limited within banking sector and other private sector organization are further gaining pace.

It needs more maturity and experience in context of adapting the various international standards. Establishing international cybersecurity norms is an essential step in protecting national security in the modern world and maintaining trust in services provided online.
Cyber security Norms are needed to address short of conflict scenarios.

There has been a lot of issues raised as recently there was a Banking theft that created a stir in the banking sector of Nepal where there is more provocative measure are taken by the central bank to ensure the proper maintenance of the system and cyber security norms.

http://internetgovernancediplomacy.blogspot.com/2017/11/nic-swift-cyber-hacked.html

BPF cyber security IGF 2018

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?

The best way is the open and clarity in terms of creating a multistakeholder environment of consultation in adapting and mitigation process which helps to create better solution.

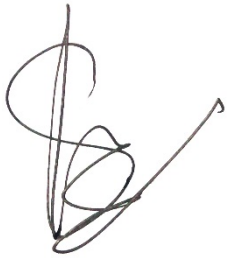
Do you have examples of norms that have failed (they have not seen widespread adherence), or have had adverse effects (living up to the norm led to other issues)?
The lower and developing nations are just working their way, I think in most of the countries the overall process of standardization has a huge challenge of multistakeholderism where cyber security is one of the hottest topic that comes up. It more like evolving where new standards and norms are also coming up which needs to be guided by better core values.

What effective methods do you know of implementing cybersecurity norms? Are there specific examples you have seen, or have had experience with?
Some norms emerge spontaneously without any particular actor having any particular intent and then become entrenched through habit. In any group that interacts regularly, norms develop simply through expectations shaped by repeated behavior. Much of the foundational engineering of the internet involves this kind of path-dependent norm development.

The most effective method of implementing cybersecurity norms would be through public dialogue process like national internet governance forum and other policy development process which provides a better platform and situation of understanding and mitigation of the problems and challenges.
Another way can be understanding the problem or challenge of cybersecurity and doing a proper research in opening up the process for dialogue in a multistakeholder environment for policy development process and can create better solution.
During the wanna Cry Virus attacked there were various collaboration seen in terms of creating a proper cyber security norm and mitigating the problem.

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?
I think there is certainly a control over the technology and with the growth and advancement digital security divide is certainly growing. From developed nation to developing to lower economies the cyber threats are also leading to a new form of digital divide, between the security ‘haves’ and the ‘have nots’. The discrimination and the differentiation has certainly created a gap in between the economies where there is tussle of having the latest and controlling the network. The whole process of divide starts at local level where the regulator wants to control the traffic. At ISP level the engineers create their own barriers and at regulation level the police want to surveillance the network. The network is never free from assumption of attack of control whether it’s the local or international the risks are the same where internet freedom and individual security is always at risk. In lower economies users who lack the skills, knowledge and resources are vulnerable to cybercrime and hacking where addressing this digital security divide will be critical to realizing the full potential of the future Internet. The gap may be the

issue but developing a basic standards is the ultimate goal where priorities needs to be set in.



Shreedeep Rayamajhi
ICT4D Consultant
Founder
Rayznews|Learn Internet Governance
https://icannwiki.org/Shreedeep_Rayamajhi