BPF on Cyber Security 2018 Contributions

1. How do you define a culture of cybersecurity?

Cyber security is the technique of protecting computers, networks, programs and data from unauthorized access or attacks that are aimed towards exploitation. Culture refers to the way of thinking, behaving and working of an individual in an organization. Cyber Security culture can act as defensive strategy to guard against cyber threats. To develop the culture of cyber security, the organization should not only depend on the IT department but to everyone starting from the senior management level to each and every staff member of the organization. This culture can be inculcated by making everyone feel that cyber security is their own responsibility, train them to provide an awareness of cyber security, make it an engaging activity and reward and recognize those who are actively involved in it.

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

Business environment is rapidly changing. Technology and services also change and evolve rapidly. This fast growing environment has started posing security problems in the cyber space and that has started to grow exponentially. To curtail this it is necessary that norms need to be developed and the norms proposed must consider the future prospects. Laws and Norms help us to secure the new environment of the current cyber space. Though there are few norms existing, more norms can be developed by entrepreneurs to protect the cyber space in terms of encryption, back doors, and the removal of child pornography, hate speech, disinformation, and terrorist threats. Though this is going to be a long process, the progress can take place simultaneously.

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.

Yes, within my field of work, I could see organizations stand up and promote specific cyber security norms. Organizations with information security department can stand up and promote specific cybersecurity norms. There are lot of proposals that has been putforth by the government, academia and civil society at the state and national level. Few of the norms that are

recently proposed are: Code of Conduct drafted in the year 2015 by Shaghai Cooperation Organization, Government proposals, agreement between the United States and China regarding cyber-enabled theft of intellectual property, law enforcement collaboration, and other cyber security measures.

From the technical perspective, the private sector has been analyzing the attacks and its origins for many years in defending the online environment There are several global ICT companies, including Microsoft, that have adopted policies and practices designed to alert users of popular online services when it appears that nation-states have targeted them.

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?

The cyber security norms developed by RBI(Reserve bank of India) towards digital transactions has proved to be successful to some extent. Recently the Department of Information Technology in India is closely working along with RBI to further enhance the security levels to defend cyber risks. It has come out with an Audit Management Application portal to handle various supervisory functions of the cyber security and information technology examination cell in the Reserve Bank and to fully automate monitoring of returns has been envisaged inorder to facilitate consistency and efficiency of the offsite monitoring mechanism. Inorder for a norm to be successful following tips could be useful:

i) The cyber security which is already implemented in other organizations should be identified and a framework can be created to be applied to organizations.

ii) Form a strongest possible working team to improve the security.

On 6 February 2018, the international 'Safer Internet Day', European Union Agency for Network and Information Security (ENISA) published a report providing organizations with practical tools and guidance to develop and maintain an internal cybersecurity culture. They identified good practices from the organizations that have already implemented cybersecurity culture programmes. These tools could also be used for enhancing the cyber security levels of an organization.

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)?

Recent issue of norms failure during the year 2016-2017 is one good example that indicates the importance of devising effective norms for cyber security. The Group of Governmental Experts (GGE) of Information Security convened by the United Nations that concluded its last round of deliberations and reported that Group appears to have failed to arrive at a consensus outcome report.

The 2016/2017 Group was tasked by the UN General Assembly to study the existing and potential threats to information security and measures to address norms, rules, principles and capacity building and over the course of a year experts from 25 countries joined together to work on it. The major study of the group was on "how international law applies to the use of information and communications technologies by states." This has led to the failure of the norm as few participants did not seriously engage on the mandate on international legal issues and this has prevented the conclusion of a consensus report.

Therefore constructing a new norm is difficult and not an easy task. Sometimes conflicts exist or compromises exist. This may lead to the failure or success of any upcoming norms. If the norm is perceived as a burden or obstacle, it will likely be ignored by the employees. It is important to examine the current cybersecurity culture with regard to the strength and weakness to avoid the adverse effects.

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

i) Carry out the research regarding cybersecurity.

ii) Collect technical reports from the cloud server and academia as well as journal publications regarding cybersecurity.

iii) Cybersecurity culture programs can be initiated among the organizations who want to adapt the change and to become most successful.

iv) Through awareness programs, webinars, brainstorming and training sessions.

iv) Cybersecurity framework can be developed.

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?

Digital Security divide is the gap between the demographics and regions that have access to the latest Information and Communications Technology (ICT). ICT plays a major role in the global economy. Smartphone penetration is considered to be the main driver of digitization in developing countries. This is primarily because smartphone devices have smart applications to achieve a particular use-case. Language also serves as a barrier in the rural market. Rural citizens use their mobile devices in their regional languages. According to the World Development Report 2016, "The internet unites people; its governance divides nations". According to me the Digital Security Divide is not the sole responsibility of the people or the country but both.

Dr.N.Sudha Bhuvaneswari
Associate Professor
Dr.G.R Damodaran College of Science
Coimbatore, India