BPF on Cyber Security 2017

Naveen K Lakshman

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)?

Internet is an Open Highway of Information, which works on Trust basis. A safe digital framework brings communication in the Internet better. Good Cyber Security ensures equality of all stakeholders which support the Sustainable Development Goals (SDGs). Technologies deployed in the Internet must not leak, steal, abuse and hijack contents that users send. We need safer communication channels , adopt to secure tools and mechanisms to keep the Internet working.

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)?

Internet works on a Trust basis, 99% of the users don't understand and bother of the Technologies that make the Internet works. A Poor Cyber Security will keep the users at Large from using this platform for communication. A better framework on Cyber Security can bring the trust to the users at Large.

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:

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

  DoS and DDoS mitigation process must be adopted. Strict laws must be framed to punish the abusers.
- Security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfill critical goals such as payments

  Mobile devices are less secure compared to PCs and Laptop, very less users are aware of the vulnerabilities of using Mobile for Online Payments. Downloading Apps for Online Payments must be from a reliable source, keeping in mind some Apps might contains Trojans, Worms. Use of HTTPs is highly recommended.
- Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended

  Most Governments around the World have been put Internet Users on surveillance. In most cases Browsing patterns of targeted Internet users are collected, potentially abuse them especially this have been done on Civil Society Rights group.
- Confidentiality and availability of sensitive information, in particular in medical and health services

  HIPAA (Health Insurance Portability and Accountability Act) adopted by the United States provides data privacy, security consideration and access to medical records is very well known act, all Government stakeholders must implement their own Privacy/Security laws for preventing misuse of patients medicals especially by Insurance Companies.
- Online abuse and gender-based violence

Online abuse in most cases Local Governments needs to contact the Website or Social network platform which takes a lengthy process. Tracing and punishing the abuser in a fast track will to an extend reduce online abuse. Revenge Porn has been a common crime which prevails the internet, any objectionable content needs to be immediately removed when requested.

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

Deploying DNSSEC for protecting the DNS Infrastructure, outreaching to all stakeholders regarding the KSK Rollover 2017. Creating awareness among the community about the necessity of deploying DNSSEC. IXP can protect their infrastructure by deploying Resource Public Key Infrastructure (RPKI).

- Vulnerabilities in the technologies supporting industrial control systems

Indentify old & vulnerabilities within the Industrial Control Systems (ICS), listing them so as the all the stakeholders are aware of the state of vulnerabilities. Patches and Firmware must be updated to reduce and fix vulnerabilities. Malwares, Worms, Backdoor, Trojan must be blacklisted.

- 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

Internet of Things (IoT) are gaining momentum, primary concern about Privacy , Interfaces for access, Security of these systems are very less researched areas. Transport encryption must be adopted for all Smart Internet devices. IoT can be compromised due to lack of security implementations, proper security auditing must be performed on IoTs deployments.

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

  All Deployment Process must define security related documentations and must consider assessing, identifying weakness of the system.
- Unauthorized access to devices that take an increasing role in people's daily lives

  Create an awareness among the Community, that Privacy and Security are his/her fundamental right. If compromised, it needs to be legally challenged.
- Other: describe a cybersecurity issue critical to developing the SDGs in ways not listed above relevant to your stakeholder community (100 words or less)

  Cryptocurrency, Bitcoins needs to be brought under the Cyber Law, in most Ramsonware attacks, victims are forced to pay a ransom using Cryptocurrency, Bitcoins which is very less traceable.

- 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?

  All stakeholders must actively participate in ensuring Cyber Security, which needs to be addressed as a Major concern in current growing Internet Infrastructure. All stakeholders must engage with the Technical Community, standards organization like IETF, IEEE, ITU, Incident Response groups like FIRST, CERT, Network

Operators Group and Internet Registries must participate with other stakeholders to bring a balance in framing a Cyber Security Policy.

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

  Cyber Security used to a topic of discussion within the Technical Community, now all stakeholders must actively participate in Cyber Security related discussions this will enable the forum to bring consensus on what need to needs to addressed to reduce and resolve the Cyber Security related issues. A framework for Cyber Security must be drafted, best practices must be adopted for implementation.

- 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?

  DoS/DDoS Attack, Ramsonware, BGP/IP Prefix Attacks, DNS abuse are the most Critical Cyber Security issues that needs to be solved. The Technical community being the major contributor for Cyber Security, should provide support and create awareness among all stakeholders. Implementation of Resource Public Key Infrastructure (RPKI) for preventing BGP/IP Prefix Attacks and DNSSSEC for protecting DNS Infrastructure must be priority topics to be addressed.

Submitted by:
Naveen K Lakshman (Technical Community), India
Email: naveen@protocol41.net