Internet Society
India Chennai Chapter

Response to the IGF Best Practices Forum on Cybersecurity Questionnaire Sep 2017

Cybersecurity is inseparable from Security of the world we live in. Cybersecurity issues and measures are a reflection of the global security issues and measures. Conversely, it is also true to the extent that any issues that arise on the Internet and the measures adopted spill over to everyday life.

It is understood that it is becoming increasingly necessary to strengthen government processes, yet parts of these response to questions on Cybersecurity strive to argue for a balance. This argument is not contrary to the understanding that governments ought not to be weak against other powerful forces, legitimate or otherwise.

It would result in significantly positive changes if the questions surrounding Cyber Security are approached with an overarching inquiry on ‘How secure is Security? Who does Security secure? The common man? The world? Or does it Secure some from many? and, Can we trust Trust?’ but the response is rather along the guidelines provided in the questionnaire.

With good Security, and uncontaminated Trust, yet with the right measure of attention to problem areas by fair means, Internet would be more fertile ecosystem.

Questions:

1. 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)?

Cybersecurity (good practices, laws and other measures) could either contribute to the growth of trust in ICTs and Internet Technologies or, unintended, cause to erode trust in the Internet. “Good” Cybersecurity is that which addresses the current issues with a profound understanding of History and resolves issues without reversing the historical progress in the timeline of our evolution. Good cybersecurity is security in the right measure, security by just and fair means irrespective of short term temptations to act on the contrary. Good (cyber)security is security that is unobtrusive, mostly supportive, perhaps even servile (in a higher sense) rather than high handed, without explicit or implicit harm, without any harm that may manifest in the present or future.

“Good” cybersecurity, with a good global blueprint and right policies would nurture good Internet technologies without prejudice, while not-so-well-thought-of invasive technologies could sideline good Internet technologies. With a good security blueprint, all good technologies would be fostered, ICTs and the Internet would evolve further as the trust in the technologies would increase.

Trust as sometimes engineered into the Internet is illusory. “Trust” can not be a euphemism. Trust, if engineered, must be honest, total and free of strings. Internet needs to be an eco-system where Internet enterprises on the progressive track, such as, Google would guard user data and facebook would defend user’s privacy, which they do to a large extent, but with enforced compromises, sometimes compromised to a degree far greater than necessary and often even when the need or circumstances are not extraordinary.

Sustainable Development goals, or any Development program, in the process of definition, debate and adoption, and in the phase of implementation, sometimes get misoriented towards programs that tend to politically, and, more often than not, commercially benefit a few interests. Good cybersecurity would ensure a fair Internet ecosystem which would bring up good and diverse ideas in the Internet space, bring together diverse players from across stakeholder groups and would cause to contribute to Sustainable Development with clear goals and unhindered and unaltered implementation.

2. 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)?

Poor cybersecurity could mean the absence of necessary measures or poor choice of measures, some make-believe, some inadequately advised, some unfathomably harmful. In both cases, it would cause Governments to be slow to embrace Internet technologies and be less prone to trust the Internet to carry out the programs.

Not only poor security, but excessive or misplaced security measures cause the erosion of trust in ICTs as excessive security measures are visibly or invisibly invasive.

3. 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:

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

It requires a shift in policy so as to encourage development of truly robust hardware and software; In the case of IoT the Community could consider a sub-architecture that is free, functional and limited to the intended purpose of the device. A refrigerator doesn't have to watch videos on YouTube.

- B Security of mobile devices, which are the vehicle of Internet growth in many countries, and fulfill critical goals such as payments

Major mobile platforms may have to consider graduating from an early phase of application environment hitherto with a focus on more and more applications, to a “growth” phase of mobile application environment that is clean with certified and accountable applications that do not ask for unnecessary device permissions. This progress is to be made without altering the fundamental values of the Internet. This would largely minimise abuse.

For mobile payment, or any payment system to be secure, the focus of the (Cyber)Security Agencies ought to be more on the recipient. So long as it is ensured that the payments terminate in a legitimate account linked to a legitimate entity of minimal required repute, or terminate to a real person without alarming financial records in any country, and that, that legitimate entity or real person finally and in some manner traceably receives the payments through a bank account with a legitimate and ‘accountable’ financial institution, the diversity of occurrence of fraud online would be significantly reduced. The approach suggested here is to focus more on the receiving entities or persons, and relatively less on the individual who makes the payment. The focus on receiving entities may also be done with the focussed and limited objective of eliminating fraudulent and criminal recipients. The focus of the Security Agencies also need to be on banks and financial institutions and payment gateway operators, behind layers of Rights, who are more difficult to deal with, and ensure that only those banks, institutions and gateway operators who are peer-endorsed and of reasonable repute are encouraged to operate payment gateways or other forms of payment systems. Care also needs to be taken to ensure that the security measures do NOT in any way increase the cost per transaction and the overall banking costs of the common man and that of business entities who transact online.

These suggestion does NOT intend to touch upon block chain systems that are somewhat anonymous, whose validity, regardless of the anonymity, is not to be confused in the context of this strong suggestion on banks and payment gateways. New innovations are to be encouraged to deal with and solve persistent gaps in the existing financial systems.

The Blockchain technology needs to be fostered at an accelerated pace for solutions to problems that defy solutions.

- C. Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended

The temptation for Authorities to excessively use surveillance technologies or acquire, and store enormous volumes of data by deploying such technologies arises in part out of impatience to resolve relatively new law and order issues. Such technologies are often developed by Commercial entities, not all of whom are entirely free of narrow considerations. Harsh, weak or useless technologies are sometimes promoted. The exaggerated needs of Law and Order Agencies for Commercial data necessitate legitimate and sometimes implicit arrangements whereby the commercial exploitation of user--provided data is also tolerated and sometimes

even encouraged. There are indeed ethical and relatively fair commercial entities, but there are more commercial players who are exploitative than there are fair players. The short term temptations to collect massive amounts of data need to be weighed against the fundamental values of freedom and justice and propriety.

- D Confidentiality and availability of sensitive information, in particular in medical and health services

Technologies exist whereby users whose sensitive data is stored, even on the cloud, could be empowered to consent to the use of their data, not only by blanket permission, but instance by instance. Such technologies could be identified and deployed and may also be integrated into Central databases. Standards are to be established to limit business access and any replication for health-profiling for business.

- E Online abuse and gender-based violence

Governments, globally, in union, by due process of stakeholder consultations, could work with the independent DNS coordination and work towards a harmless process which would, without altering Core Internet Values, work towards rough consensus on identifying extremely harmful and nefarious content online and seek a community process of judgement to identify and eliminate/discourage content that is overwhelmingly and extremely harmful or nefarious, with care and high level oversight to ensure that such a process is not captured by any stakeholder or powerful interests and abused for political or commercial reasons.

Gender violence (or child abuse) is a global issue, it is real, but the visibility of this issue is disproportionately magnified on the Internet. The issues are better addressed more comprehensively as a global ground reality issue, in the right measure, than merely as Cyber Security concerns. While addressing these issues, it may also be noticed that the hype about gender violence or child abuse is also suspect, to the extent that these issues, among all the global problems, gain far more visibility due to the fact that these are issues that capture people's attention, and any measures formulated and implemented in the name of prevention of gender violence or child abuse are prone to accepted without due scrutiny and sometimes get implemented to achieve possibly unseen intentions. These are issues of popular appeal, and deeper scrutiny on a higher level is required to examine the politics, if any, behind these issues.

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

The Domain Name System, like the Internet, is young. The DNS has been instituted well, and it is evolving very well. As it evolves along its instituted framework, the DNS would by itself address the security risks one after another and would assure the Security and Stability of the Internet.

Internet Exchange Points were envisaged to be dumb and neutral, but intelligence is increasingly built into the exchange points, by commercial aspirations and possibly encouraged

by political directives. The security risks of Internet Exchange points arise from the very security measures which have encouraged an increasing number of Internet Exchange points to introduce intelligence. It would be in the interest of Governments to ensure that the exchange points remain neutral and ‘stupid’.

- G Vulnerabilities in the technologies supporting industrial control systems

Vulnerabilities are present by careless design or wilful design. A long term solution would to be debate on the wisdom of treating the Internet of Things (the term is used here broadly to include industrial equipment) as different from the “Internet of people”, a term coined to strike a distinction from the Internet of Things. If it is wise, there could be an IoT architecture that would limit access to “Things” by those who do not have a business to access them. In the short term, the solution lies in working towards common standards that even Proprietary designs could adopt, and by favoring device manufacturers who adopt common standards.

- H 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

It requires some globally agreed upon principles for collection and use of data. Part of the harm resulting from the repurposing of data could be minimised by first limiting information gathered by IoT to what is barely necessary. Smart meters, for instance, need to have smartness only to the extent that is rational and justified.

By definition, if any data is ‘improperly’ anonymized, it is bound to be de-anonymized. Part of the solution to the problem of deanonymizing improperly anonymized data lies in limiting access to any anonymous data ever collected.

In the process of collecting, anonymizing, storing, using and sharing citizen data the Governments need to be uncompromising in setting standards and processes.

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

The pace of evolution of these technologies is so fast that there is a short time gap between development of the technologies and the creation of suitable secure development processes, but eventually it would get streamlined.

- J Unauthorized access to devices that take an increasing role in people’s daily lives

Part of this occurs by enabling unauthorised access by design, as a security measure which in turn causes more grave security issues.

4 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?

The development of Internet technologies is widely dispersed, but technologies so developed become part of the global Internet. The development of standards, and the coordination of the critical resources or functions occur by the multi-stakeholder process which is evolving as the most suitable form of governance of the Internet. While the strengths are being increasingly acknowledged, Governments perceive risks in the process of coordination or governance being remarkably different from the established models of governance. The risks perceived are somewhat exaggerated.

Many Governments are still hesitant to embrace the multi-stakeholder process for Security policy-making as reflected accurately in the views expressed recently that “Internet Governance is a multi-stakeholder process, but Security is a Government subject”. This thinking is slowly broadening to gradually embrace the multi-stakeholder process for the whole of Internet Governance without reservations. As this happens, the broader CyberSecurity policies could be shaped by all stakeholders, while Strategies to deal with specific threats or the details of responses to specific incidents could be by duly ‘weighted’ stakeholder representation in the process, under a very high level multi-stakeholder oversight, with as much ‘weight’ reserved for Government Agencies as the gravity of the threats warrant or when the sensitivity for secrecy of the strategies is high.

The arguments for opening up the sphere of (Cyber)Security Policies and Implementation to multi-stakeholder process could be summed by pointing out that the Government-only process still preferred by conservative Governments is not in reality a Government-only process but actually happens to be an inevitable Government-Private process, or a partnership. It is a “partnership” in Nations where there are strong Governments, and a captured process where there are weak Governments, all of which is largely unacknowledged. In CyberSecurity, which overlaps and spills over ground-level Security, even in matters of National Defense of its borders, the infrastructure development and the program implementation requires an overwhelming level of Business expertise and participation, and such a partnership invariably progresses to strengthen business interests rather than the other way around. (History records a pattern wherein the commercial entities gain dominance whenever there are inevitable or necessitated partnerships between Sovereigns and Business.) Broadening this existing, but unacknowledged model of Public-Private partnership by including an additional stakeholder class (Civil Society / Internet Community / Academic Community), at least as one additional broad class of stakeholders, perhaps even as distinct additional groups of stakeholders, would benefit the Internet and the World immensely by bringing about a balance in the process of

CyberSecurity and all Security decisions. The multi-stakeholder process would ensure that Security policies evolve with fairness and that there are no misdirection or underlying private aspirations in framing a certain policy or decisions on the measures.

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

The role of Governments in the multi-stakeholder process is to unconditionally enable the process itself, make resources available, implement / enable implementation, govern or facilitate as may be suitable in varying situations concerning CyberSecurity.

The role of Business would be to advise on suitable solutions, offer the necessary commercial support as needed. The business of business is to pursue profits and it would be fair for this stakeholder group to have fair commercial pursuits in the process of fulfilling the need for solutions. The more fundamental role of this stakeholder group is to first ensure that there is fair representation, not necessarily geographically, within the stakeholder group so as to play a fair role.

The role of Civil Society, Academic Community and International Organizations would be to identify, research and develop suitable technologies and standards, and contribute by diverse thoughts to help evolve balanced Security policies. The role of this stakeholder group is more importantly to articulate the needs and concerns of the average Internet user and seek such solutions that would not harm the most fundamental values and the Core Internet Values or otherwise cause a reversal to the world's progress towards freedom.

6 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?

The most critical cybersecurity issue pertains to the global issue that has been persistent over the last 25 years, which is that of extreme threats. The threats have been so dire that the measures taken to deal with the threats have altered the way the common man lives his life. By the correspondingly extreme processes and measures taken to solve a 25 year old problem, the progress made over millennia has been somewhat reversed. The stakeholders may be invited to identify solutions that would effectively deal with this critical issue in the right measure without altering the way we live our lives.

Sivasubramanian Muthusamy
President
Internet Society India Chennai

http://isocindiachennai.org @isocchennai isocindiachennai@gmail.com 6.Internet@gmail.com