2017 Best Practice Forum on Cybersecurity
UN Internet Governance Forum Intersessional Work

The Internet Society (ISOC) is committed to the enhancement of online trust and making the Internet available to everyone, everywhere. For twenty-five years, we have worked collaboratively with our global community and diverse stakeholders across the globe to advance Internet growth and promote its open development, evolution, and use for the benefit of all people. As one of the organizations involved in the WSIS discussions since its inception, the Internet Society has actively engaged in the IGF process. Therefore, we are pleased to submit our contribution to the ongoing intersessional work from 2017 IGF Best Practice Forum on Cybersecurity, addressing the following questions from the call for contributions:

Question 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)? / Question 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)?
For the first time, the UN acknowledged Internet access as a key part of implementing the global Sustainable Development Goals (SDGs), through SDG 9C - *'Significantly increase access to information and communication technology and strive to provide universal and affordable access to the internet in least developed countries by 2020'*.

Access to an open, trusted Internet changes lives. It can help to alleviate poverty, fight inequality and injustice, tackle climate change and help kids get an education. The Internet Society's approach for an enabling environment for Internet growth and development is based on building connectivity, communities, capacity, and infrastructure policies. We are committed to an Internet for everyone everywhere; "free from censorship, unhindered by over-regulation, an enabler" of progress. An Internet that can build a business from "a spark of an idea, educate the most remote communities," protect human rights and drive economic and social development. Internet access needs to be open, affordable, reliable and relevant to be meaningful and offer opportunities for a sustainable development.

The Internet needs a solid foundation in trust for its full potential to be realized. An 'open and trusted Internet' is a globally, distributed, interoperable network of networks that cultivates innovation and creates opportunities for all. Its foundation lies in user trust, technologies for trust, trusted networks and a trustworthy ecosystem.[1] It offers inclusive governance, is built on sound policy principles and strives to put the interests of Internet users at the heart of decisions.

All stakeholders have a positive role to play in nurturing a trusted and open Internet. We need to work together to secure core aspects of Internet infrastructure, to protect the confidentiality and integrity of the data that flows over it, and to ensure the right policies are in place to support the technologies, networks and actors that make the Internet work. We do this through collective responsibility and collaboration.

The Internet Society invites policymakers to use the Internet Society's policy framework for an open and trusted Internet as a guide for addressing the complexities of building trust in an open environment such as the Internet.

Question 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: *Denial of Service attacks and other cybersecurity issues that impact the reliability and access to Internet services/ Security of mobile devices, which are the*

[1] Internet Society Policy Framework for an Open and Trusted Internet, https://www.internetsociety.org/resources/doc/2016/policy-framework-for-an-open-and-trusted-internet/

vehicle of Internet growth in many countries, and fulfill critical goals such as payments/ Potential abuse by authorities, including surveillance of Internet usage, or the use of user-provided data for different purposes than intended/ Confidentiality and availability of sensitive information, in particular in medical and health services/ Online abuse and gender-based violence/ Security risks of shared critical services that support Internet access, such as the Domain Name System (DNS), and Internet Exchange Point (IXP) communities/ Vulnerabilities in the technologies supporting industrial control systems/ 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/ The lack of Secure Development Processes combined with an immense growth in the technologies being created and used on a daily basis/ Unauthorized access to devices that take an increasing role in people's daily lives/ Other: describe a cybersecurity issue critical to developing the SDGs in ways not listed above relevant to your stakeholder community (100 words or less)

ISOC and ISOC staff have been working on multiple activities tackling some of the challenges identified above. We would like to highlight some examples as they serve as ideas for approaches that might be taken to address the identified challenges:

- **MANRS** - To create a sustainable technical and business environment, organizations must work together to address the challenges of the security of the Internet's routing system. Deploying small measures, like those defined in the MANRS Actions, can make a big difference. MANRS provides added value for the network operator and its customers: better protection against traffic anomalies caused by misconfigurations; cleaner setups resulting in easier troubleshooting and lower time-to-resolution (TTR); improved peering conditions; and opportunities for valuable collaboration with other operators through a discussion forum and professional network. Many MANRS participants go beyond these baseline actions, leading the group of participants and encouraging further collaboration.
- **AFRICAN INTERNET INFRASTRUCTURE SECURITY GUIDELINES** - The African Union Commission (AUC) and ISOC have jointly developed Internet Infrastructure Security Guidelines for Africa based on contributions from regional and global Internet infrastructure security experts, government and CERT representatives, and network and ccTLD DNS operators. The Guidelines emphasize the importance of the multistakeholder model and a collaborative security approach in protecting Internet infrastructure. They also put forward four essential principles for Internet infrastructure security: Awareness, Responsibility, Cooperation, and adherence to Fundamental Rights and Internet Properties. The Guidelines recommend the most critical actions for various stakeholders to take on Internet infrastructure security, tailored to the African cybersecurity environment's unique features. This set of recommendations is a first, yet significant, step in producing a visible and positive change in the African Internet infrastructure security landscape.
- The **Global Commission on the Stability of Cyberspace (GCSC)** launched in February 2017, comprising experts from different backgrounds and regions, "is helping to promote mutual awareness and understanding among the various cyberspace communities working on issues related to international cybersecurity". The GCSC has a clear goal of "supporting policy and norms coherence related to the security and stability in and of cyberspace", and is supported by a Research Advisory Group.
- **APAC Privacy Issues Paper** - In the latest annual survey of the ISOC community on policy issues in the Asia-Pacific, cybersecurity and privacy replace e-commerce and cloud computing in the top five most monitored policy areas in the APAC region. The survey also revealed that 59% of the respondents believe that their privacy is not sufficiently protected when they use the Internet. Building on the online privacy framework and concepts presented in the Internet Society Policy Brief on Privacy, this issues paper focuses on online privacy concerns and good practices in the Asia-Pacific region.
- **Latin America and Caribbean Anti-Abuse Working Group - LAC-M^{3}AAWG,** a regional initiative that combines knowledge and efforts from LACNIC, LACNOG, and M^{3}AAWG to develop a self-sustaining anti-abuse community in the LAC region. It serves as a convening forum for network operators and anti-abuse experts. LAC-M^{3}AAWG's mission is to foster dialog among existing communities and working groups, promoting the development of anti-abuse recommendations and best current operational practices (BCOPs) that address region-

specific and global issues. It will also act as the voice of the LAC region in the global anti-abuse community, further cementing the exchange of anti-abuse ideas, knowledge, and best practices between the LAC region and M[3]AAWG's global community.

- **The OTA 2017 Online Trust Audit and Honor Roll** represents the 9th year that the Online Trust Alliance (OTA) has conducted benchmark research to promote security best practices, data stewardship and responsible privacy practices. The primary goals of this work include raising the level of data security and privacy, while recognizing organizations that have demonstrated security and privacy excellence. In addition to the Honor Roll status, this year's Audit includes the "Top of Class" representing the top 50 organizations based on their total score. The 2017 report also reflects OTA becoming part of the Internet Society (ISOC).
- The **Internet Society's Anti-Spam Toolkit** is part of the joint work with ITU and other partners to address the challenge of spam for Internet users, businesses, and policymakers alike. It provides resources for governments, network operators and users, including an online module about combatting spam and mobile threats, and policy briefs about botnets and spam, with policy recommendations.

Question 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?

All stakeholders have a positive role to play in nurturing a trusted and open Internet. We need to work to secure core aspects of Internet infrastructure, to protect the confidentiality and integrity of the data that flows over it, and to ensure the right policies are in place to support the technologies, networks and actors that make the Internet work. We do this through collective responsibility and collaboration.

A useful foundation can be found in the principles of Collaborative Security: fostering confidence and protecting opportunities; collective responsibility; fundamental properties and values; evolution and consensus; think globally, act locally.

The Internet Society's policy framework for an open and trusted Internet outlines an approach for addressing the complexities of building trust in an open environment such as the Internet. It is described through four interrelated dimensions of trust that need to be considered when developing policies for the Internet, and provides principles to build a trusted Internet. This framework for a trusted Internet embraces the important and valuable differences that give our world its rich diversity.

There is no 'one size fits all' solution to decision-making about the Internet. Pro-Internet policies can take many different shapes, matching each country's unique needs. But one thing unites them all; their starting point is '*how do we build trust in an open environment such as the Internet.*'

Question 5 - 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 Internet of Things (IoT) is a rapidly developing industry sector. With massive investments from industry, the number of connected "things" is expected to drastically grow in coming years[2]. Unfortunately, as is often the case with fast-paced developments, IoT security is falling behind. We have

2 Gartner. "Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016." http://www.gartner.com/newsroom/id/3598917

experienced massive distributed denial of service (DDoS) attacks fueled by botnets made up of insecure IoT systems[3]. We have also seen IoT devices be hacked, and users lose their personal data[4]. Today, price and time to market take higher priority over security and privacy for many manufacturers and service providers in the IoT ecosystem.

We need stakeholders, particularly the developers of IoT systems, to recognize security and privacy *by design* (i.e., as part of their design processes from the beginning, rather than "bolted on" at the end as an afterthought) as the most important features of an IoT system, and to consider the long-term "sustainability" of their offerings in light of security and privacy[5]. IoT security must be taken seriously by all stakeholders, and addressed to safeguard users, maintain trust in the Internet, and protect the opportunities promised by IoT and the Internet. With the cyber and physical worlds rapidly converging through the expansion of IoT, the scope of the dangers posed by IoT insecurity are also mounting. Never before has the virtual world penetrated so deep into our physical lives, and if security goes unaddressed, we are risking not only user confidence in the Internet, but also the physical safety of individuals. However, addressing security challenges must be done while preserving the fundamental drivers of the Internet. For example, in some cases requiring too rigorous security requirements for devices may stifle innovation and development, while addressing system wide security is a more appropriate and long-term strategy.

IoT security is hampered by a lack of commercial incentives. For IoT manufacturers and service providers, good security is expensive, requires particular skills which may not be readily available, and security-by-design slows a product's time to market, which is a major factor in this very competitive environment. These stakeholders also do not bear the majority of the costs of an attack in many cases; instead, this falls on the consumer. In turn, consumers have trouble buying secure products, as they have little to no means of distinguishing between a secure and insecure product. They also may value price or other attributes higher than security when purchasing IoT products.

It is also important to note that IoT is not only devices, but an ecosystem made up of individual IoT systems that include physical devices, software, servers, the communications between individual parts of the system, and more. Every part of an IoT system must be secured[6]. Therefore, there are many parties with a stake in security[7] including: Vendors of sensors and actuators (devices); Middleware developers; Application developers; Protocol developers; Middleware operators; Application services operators; Device manufacturers. In many cases, manufacturers use components sourced from other vendors, and the security characteristics of those may be difficult to evaluate. Outside the technical realm, the number of entities is also significant: Retailers and resellers; ISPs and service providers; Insurance companies; Policymakers and regulators. And we should not forget another important "stakeholder" – the user, be it an organization, municipality, government, or individual. Consumer choices define how valuable security features are.
Every stakeholder has both a stake and responsibility in securing the IoT ecosystem[8]. It will be critical to bring these diverse stakeholders together to address the pressing issue of IoT security[9]. No individual stakeholder can tackle the issue on their own.

---

3 Kerbs, Brian. "Hacked Cameras, DVRs Powered Today's Massive Internet Outage." https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

4 Franceschi-Bicchierai, Lorenzo. "Internet of Things Teddy Bear Leaked 2 Million Parent and Kids Message Recordings." https://motherboard.vice.com/en_us/article/pgwean/internet-of-things-teddy-bear-leaked-2-million-parent-and-kids-message-recordings

5 See the Online Trust Alliance's "IoT Trust Framework" for more best practices for IoT manufacturers and service providers. https://otalliance.org/system/files/files/initiative/documents/iot_trust_framework6-22.pdf

6 See our blogpost, "There is no Perimeter in IoT Security" by Andrei Robachevsky https://www.internetsociety.org/blog/2017/06/there-is-no-perimeter-in-iot-security/

7 See the Online Trust Alliance's document, "Internet of Things: A Vision for the Future" https://otalliance.org/system/files/files/initiative/documents/iot_visionforthefuture_0.pdf

8 See our document, "Collaborative Security: An Approach to Tackling Internet Security Issues." https://www.internetsociety.org/collaborativesecurity

9 See the Online Trust Alliance's document, "Securing the Internet of Things: A Collaborative & Shared Responsibility" https://otalliance.org/system/files/files/initiative/documents/iot_sharedrolesv1.pdf