Background Paper – IGF 2015 – Cybersecurity and Trust

#security #privacy #trust #multistakeholderism #governance

Managing security risks for sustainable development

Today's cyber security trends are evolving at an overwhelming pace, posing an ever-present threat to our connected world. Many leaders and decision makers in public and private organisations are realising that in addition to being a driver for innovation, productivity and growth, the digital environment also introduces uncertainties that can jeopardise economic and social prosperity. Digital security incidents can have far reaching economic consequences for organisations, for example in terms of disruption of operations (e.g. through denial of service or sabotage), direct financial loss, lawsuits, reputational damage, loss of competitiveness (e.g. in case of theft of trade secret), as well as loss of trust among their customers, employees, shareholders and partners.

Public and private sector organisations are progressively recognising the scale of the challenge and the complexity of creating a more secure Internet environment in an open globally-accessible decentralized Internet. IGF is the platform to start building a common understanding on these issues, where different stakeholders can have their perspectives heard in a not-binding and less-contentious manner. This workshop aims to highlight two main elements:

First, the global interconnectedness of the digital environment creates interdependencies among stakeholders. Interdependency has positive aspects such as enabling economic and social benefits for each based on the collective power of everyone. It has also drawbacks, such as increasing complexity, facilitating the propagation of threats and vulnerabilities, and potentially increasing collective risk. In such a highly interconnected environment , security risk management necessarily becomes a shared endeavor –based on broad participation and an approach that considers the overall security and resilience of the Internet and its actors, not just one's own security risks.

Second, at a global and individual level, while everyone talks about "cyber security," they often do not all mean the same thing. Perspectives on cyber security are far from uniform, for instance:

- Businesses need to safeguard customer information, protect commercial data, or prevent intrusions and damage to their corporate networks. Small companies and large companies face very different security issues.
- Users want to be secure and feel threatened about the effects of leakage of personal data.
- Governments have to take into account the concerns of citizens and businesses while also dealing with any national security threats that an Internet attack might pose.
- And, there are differences between developed and developing countries in how they address cyber security. While developed countries might be most focused on securing advanced computing infrastructure or funding cyber security R&D, a

developing nation might well be more concerned with developing the technical and policy capacity to deal with online fraud.

It is the legitimate claims of all of these stakeholder groups that explain why it is so difficult to reach consensus on how to define or address cyber security. Any framework for tackling cyber security needs, therefore, to work from an understanding of the different ways in which the Internet is valuable to its different stakeholders. This is reflected in the Internet Society's approach to the development of cyber security policy initiatives.

The draft OECD Recommendation on digital security risk management for economic and social prosperity, also recognizes that effective policies cannot be unilaterally created by government and that all stakeholders must work together. Security is not achieved by a single treaty or piece of legislation; it is not solved by a single technical fix, and a purely technical approach is insufficient to manage digital security risk. In this context, a principle-based framework is, therefore more beneficial than a rules-based framework. Principles are general statements that define a goal or objective of the entity adhering to the principle. In the case of information or cybersecurity, the main constituent of a principles-based approach is a risk management approach. The main advantage of a risk –based approach is that it can cover a wider range of scenarios than rules-based approaches.

In addition, a risk management approach recognises that it is impossible to create a "safe and secure" environment, whether online or offline, and therefore that a certain level of risk has to be accepted to carry out economic activities. Thus its objective is to assess and treat (or mitigate) the risk in order to lower it to an acceptable level, according to the economic objectives at stake and the context.

Finally, the establishment of a holistic and systematic digital security risk management approach can create the conditions for risk to be managed together with opportunities, and to more comprehensively take into account the legitimate interests of others, as well as the potential impact of security measures on human rights and fundamental values, and on the digital environment.

Various methodologies, standards and best practices can assist in carrying out risk management. They can help at many levels, with respect to the overall process as well as for specific aspects such as security measures or preparedness.

However, the bulk of public and private organisations, and in particular Small and Medium Enterprises (SMEs), are not yet ready to manage digital security risk from this perspective and still consider this issue as mainly technical.

In this light, panellists will be invited to explore the meaning of cybersecurty, implications for different stakeholder groups and challenges for a common understanding and management of risks.

This workshop will build on previous IGF and WSIS+10 discussions (http://www.internetsociety.org/no-106-cybersecurity-throwing-out-preconceptions and https://www.unesco-ci.org/cmscore/52/52-cybersecurity-%E2%80%93-searching-common-understanding) and aims at allowing stakeholders to share their thoughts and recommendations on managing security risks for a sustainable and inclusive development.