ACSIS CONTRIBUTION TO BEST PRACTICE FORUM

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)?

The rapid growth and adoption of ICTs as a key driver of the economic development would be jeopardized if measures to protect connected devices and user generated data is absent. The fear of data compromising, information theft, privacy intrusion, surveillance, unreliable software programs and applications would not allow those unconnected billion people to fully rely on the use of the internet and its related technologies therefore distant the realization of sustainable development goals.

The emergency of internet, penetration and its usage was given highest consideration with less attention to its security issues. Less attention to protecting the information and communication technologies and internet technologies would lead to high rate of disadvantages over the benefits.

Abuse of the use of technologies would be on the increase on a daily basis as there is or little comprehensive short rules backing the usage of such technologies. Reliability and authenticity of information will be rendered useless and reduction in innovation of business services

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 service

The policy option to address the issues of cybersecurity should be a clear awareness of the potential impacts, rules and action to guide against such acts

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

Technologies products and services should undergo through the testing stages to ensure compliance to standards and bug fixes. Also, there is a need for penetration testing at every stage of technology products and services

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

In the fight to secure the online environment, authorities somehow has violated and abuse the openness of the internet and user privacy. To help address the abuse, clear formulation of a set of rules on data respect and user privacy should be enacted.

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?

Joint efforts to the formulation of cybersecurity policies to protect the internet technologies and ICTs would help ensure and prevent hindrance to internet development. A periodic evaluation of cybersecurity policies, issues and forum where all stakeholders on an equal footing to address and resolve any potential changes and development. Also, a careful and sensitive approach to defining requirements and measures need be; to avoid strict measures which could jeopardize the future of internet development.

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 issues is the vulnerability of critical infrastructure and internet resources. Recent development has seen attacks on infrastructures to disrupt transmission and processes, to eavesdrop, and control while gaining access to useful information. The security of infrastructure and internet resources which ranges from hardware to software must be in every stakeholders mind as these formed the base for accessing user information.

Submitted by: Akinremi Peter Taiwo
ACSIS West Regional Coordinator
compsoftnet@gmail.com