Submitted by:

Opeyemi Onifade, CISSP, CISM, CISA, CGEIT, BRMP, ISO 27001LA

Managing Consultant, Afenoid Enterprise Limited

Board Member, Africa ICT Alliance

Board Member, ISACA Abuja Nigeria

Questions:

ROADMAP TO REMOVING CONSTRAINTS TO CYBERESILIENCE IN DEVELOPING COUNTRIES

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 is more than a risk management capability; it is also an economic strategy to promote digital wealth and foster trust in interactions and transactions on the Internet. e-banking, e-commerce, e-government and other e-things are possible because there is a perception that a level of integrity is inbuilt in the Internet.

Good cyber security is a means of achieving and sustaining the credibility of the Internet as a safe environment for businesses to thrive and sustain economic value. The outcome of effective cyber security will ensure that stakeholder's trust is not violated and therefore the confidence to leverage the Internet to pursue the SDG is heightened socially and economically.

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 fosters the proliferation of cyber crime, cyber hacktivism, and cyber espionage. The quantum of online vulnerabilities is a good reflection of the degree of likely proliferation of criminal activities. Criminal activities undermine the achievement of the SDG.

Policy Options to address threat scenarios

- It is important for all nations and especially developing nations to become serious about putting in place a robust risk-based Management System for cyber security that is driven by a cybersecurity strategy that enables the increasing awareness of threats and effective incident response.
- To strengthen the cyber resilience profile of the countries, there is a need to adopt a country-wide vulnerability management policy enforced through a programme which will discourage violation of intellectual property rights common with the deployment of operating system software, desktop applications and mobile applications. Unlicensed software applications are major sources of untreated security risk exposures in poor countries.
- Policies should be in place to ensure stakeholder transparency and accountability among ISP, DNS and IXP communities.

Critical issues affecting cybersecurity and the actualisation of SDGs

The following issues need to addressed for cybersecurity to enable the SDG goals:

1. Cybersecurity framework: A country needs to adopt and adapt cybersecurity framework such a ISO 27032 to ensure that there is a deliberate set of activities in place to prevent, detect and correct cyber risks. The framework should be clear on goals and metrics for determining the achievement of these goals. These cybersecurity goals could be mapped to SDGs or cascaded from the SDG.

2. Cybersecurity Processes: critical processes and practices need to be identified, established and institutionalized. Such processes include risk management, access management, process control, security services, system accreditation, and Secure Development Processes
3. Cybersecurity structure: An agency of government should be in place to own the accountabilities for deterring and recovering from cyber attacks
4. Cybersecurity culture and behavior: The educational curricula at all levels should promote acceptable behaviour in the cyberspace. Themes such as online bullying, harassment, hate speeches, privacy, etc should be clearly understood.
5. Cybersecurity intelligence and surveillance: The countries should have a means of gathering information that will help with making correcting decisions about risk exposure without violating the privacy and freedom of citizens
6. Cybersecurity practitioners: Every country needs skillful and competent people to defend her interest in the cyberspace. There should be a deliberate policy to create job opportunities in cybersecurity with attractive incentive.

7. Cybersecurity innovation: Development of cyber security products, services, infrastructure and applications should become integrated in trade promotions and innovation contest for young people.

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 UN and ITU need to develop a framework to foster international cooperation and legal principles for cybersecurity. Developing countries may require the support of ITU and the UN to **eliminate** cybersecurity blockers that are technical, organizational, or related to capacity building.