An overview of cyber security challenges in developing world

Information and Communication Technology (ICT) has assumed a critical role in facilitating social-economic development in many countries. Some countries have taken advantage of the effectiveness and productivity of cyberspace and are in the process of transforming their economies into an information and knowledge based economy. In developing world, ICT is a key component in improving the quality of life and participation in global economic activities. However, these benefits are being challenged by the increasing sophisticated cyber threats where there is no global consensus on how to regulate cyberspace. Although most developed countries have in place comprehensive ICT and Cyber security policies and plans or are at an advanced stage of implementing them, developing countries are short of the capabilities and infrastructure when it comes to cyber security countermeasures. Most hardware and software products used in the developing world are developed in the western world and without proper measures on how to secure these products, these countries are vulnerable to cyber exploitation due to inherent vulnerabilities on these products.

Cyber security is anyone business and we cannot afford to ignore the growing number of cyber threats. We live in an interconnected world and an attack to one nation could spread to other nations. While we enjoy these technologies they also create vulnerabilities to cyber-based threats. These threats arise from a wide array of sources, from business competitors, corrupt employees, criminal groups, hackers and foreign nations engaged in espionage and information warfare. Their sources vary in terms of capabilities of the actors, their willingness to act, and their motives, which can include monetary gain or political advantage among other. Last year, 5 alleged hackers were charged in the largest cybercrime credit scheme in U.S. history. The Russian and Ukrainian national are believed to have hacked 160 million credit card numbers which facilitated them to steal hundreds of millions of dollars. Other hackvist groups like Anonymous are people who are willing to launch attacks on government, religious, and corporate websites. Anonymous were earlier supporters of the global Occupy movement and the Arab Spring. Last year a group calling themselves Anonymous Africa hacked the Zimbabwe's defence, and targeted South Africa's ruling party African National Congress (ANC). Attack on individual personal data and businesses Intellectual Property could

result in identity theft, lower quality counterfeit goods, lost sales or brand name value to businesses and this in return could lower overall economic growth and declining international trade.

According to ITU ICT facts and figures, by 2014, 55% Mobile-broadband subscription are expected to be in the developing world, compared with only 20% in 2008 (ITU Website). ICT dependency in developing nations creates favourable condition for cyber criminals due to poorly secured networks, lack of cyber laws and shortage of ICT security skills. Research studies and surveys show that most computers in these nations are vulnerable and IT security awareness is below any reasonable threshold. In developing world especially most African countries, cyber security is at its earliest stages and very few countries have Computer Incident Response Team (CIRT). There is an urgent need to create a cyber security ecosystems to mesh together these elements to ensure a safer cyberspace.

While developing nations recognize the need for cyber security, many would argue that they have more pressing issues like HIV/AIDs or poverty to tackle. On the other hand if these issues are not addressed these nations could miss out on the economic benefits. Learning from the lessons of the past decade, not acting now could create a digital divide between the rich and poor countries. A global consensus is urgently needed to come up with visible plans for funding and Public-Private-Partnership with enterprises to reach fast growth of the network and the bandwidth, as well as the security level.

Cyber Security is an important part of our life today. The fact that we have interconnectivity of networks means that anything and everything can be exposed. Our critical infrastructure can be violated. Developed countries lacks well-trained cybersecurity experts. Level of understanding and education in cybersecurity issues among law enforcements agents, judiciary are not up to the standard. Developed world could help train experts who are home grown in cybersecurity.