COVID 19 and Cyber Security

Udeshika Jayasekara

Published on Colombo Telegraph on 25th June 2020

"Cyber security, referred to as information technology security, focuses on protecting computers, networks, programs and data from unintended or unauthorized access, change or destruction."
University of Maryland University College

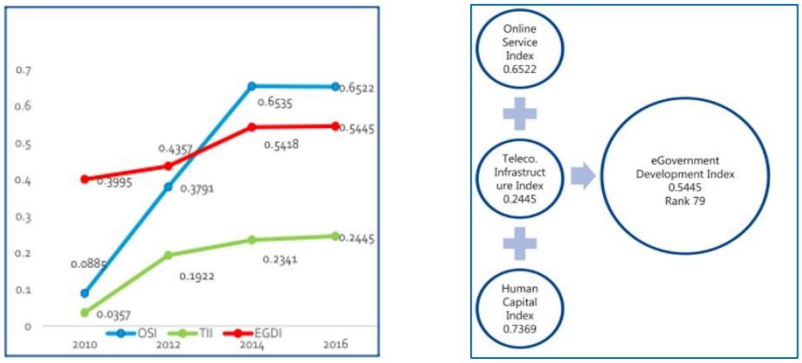
The COVID-19 pandemic created an immense humanitarian crisis that severely affected most all countries within the world. Due to the health security measures taken by the governments, it forced organizations and individuals to adopt new practices like social distancing and working from home. As a result, more and more people began to carry out their daily transactions, purchases, office administration and even for education digitally and thus became very vulnerable for cyber-attacks. Because of the COVID 19 Cyber security has become a general concern for all citizens, professionals, politicians, and, more generally, all decision makers. It has also become a serious concern for our societies that must protect us against cyber security attacks with both preventive and reactive measures, which imply a lot of monitoring, and must simultaneously preserve our freedom and avoid general surveillance. Cyber-attacks may be conducted by criminals, but also by states for industrial espionage, for economic damage to apply pressure, or to inflict real damage to infrastructure as an act of war. Sri Lanka CERT has declared that a couple of websites in Sri Lanka were defaced by a group of activists.

When considering the progress of Sri Lanka in a Digital government, Sri Lanka is ranked 79 in the United Nations e-government development index (EGDI) among 190 member countries. In 2016, Sri Lanka scored 0.6522 in online service index (OSI) which focuses on overall digital government applications 0.2445 in telecommunication infrastructure index (TII) which focuses on the status of telecommunication infrastructure, Internet facilities and Internet usage and 0.7363 human capital index (HCI), which focus on adult literacy and level of schooling. So Sri Lanka scores in the online service index and the human capital index are above the global average while Sri Lanka's score in the telecommunication infrastructure index is below the global average.

In addition, Sri Lanka has the relevant legislation, policies and standards in place now, such as Payment device frauds act in 2006, Electronic transaction act in 2006, Computer crimes act in 2007, a fully functional cyber-crimes unit at the police CID to investigate cyber-crimes and Sri Lanka Computer Emergency

Readiness Team SLCERT serving under the supervision of the Ministry of Defence. (Dias 2020)

Figure 01: Progress of the development of Digital government



Source: Sri Lanka Computer Emergency Readiness Team (SLCERT)

Due to the COVID 19 crisis, most of the government and private sector organizations were forced to work from home which was very productive provided that home computer system is also secure. Within the COVID19 period, two government sites experienced cyber-attacks. In the last ten years Sri Lanka had been subjected to several cyber-attacks when compared to last year which was only 13 this year only three up to now (Dias 2020).This was mainly due to a Task force being activated to monitor and deal with it. These attacks had taken place due to the weak construction of government websites with less concern for adapting protective security measures and due to the use of simple and obvious passwords. So to prevent such attacks in the future a sustainable cyber security method should be adopted by all institutions, companies, and government.

As social distancing policies have forced numbers of employees to work from home, and as people seek ways to stay connected, the usage of video conferencing platforms has exploded with many of the biggest companies offering a limited time free access. Zoom had a particularly dramatic growth with its user base increasing from 10 million daily users in December 2019 to 200 million in March. This unprecedented usage exposed serious privacy and security issues with Zoom. Attackers have targeted meetings and they enter a random Zoom call and screen share explicit images to harass users.

Cyber-security issues are challenging for everyone at every time more generally especially after COVID19 began. Therefore, authorized institutions and individuals should share knowledge about Sri Lankan laws and legislations on cyber security and should empower lawful bodies as fully functional professional bodies. Further, both public and private sector organizations should

circulate a natively integrated, automated Security Platform, which is specifically designed to provide consistent, prevention-based protection on the endpoint, in the data center, on the network, in public and private clouds, and across cyber environments.

Since people know the taste of digital governance now, it will definitely cause to increase issues regarding cyber space gradually. Beforehand the necessary steps should be taken to focus on prevention. Organizations can prevent cyber threats from impacting the network in the first place, and minimize overall cyber security risk to a manageable degree.

Mrs. Udeshika Jayasekara served as Research Assistatn at the Instittute of National Security Studies (INSS), the premier think tank on National Security established under the Ministry of Defence. The opinion expressed in this article are her own and not necessarily reflective of the INSS.

Bibliography

Bricata. Cybersecurity Issues Abound During the COVID-19 Pandemic. April 16, 2020. https://securityboulevard.com/2020/04/cybersecurity-issues-abound-during-the-covid-19-pandemic/ (accessed June 24, 2020). Sri Lanka Computer Emergency Readiness Team | Coordination Centre. Annual Activity Report 2019. Annual, Sri Lanka CERT, 2019. Dias, Lal. Public Lecture. "The Challenges of Cyber security in Sri Lanka." at the Institute of National Security Studies, Sri Lanka (INSSSL). June 17, 2020.