Potential Internet Risks

We can't escape technological advancements. Digital transformation has introduced a whole new experience. Technology has permitted us to enter a digital world and given us various chances. The Covid-19 pandemic brought technology more frequently into our lives. The internet has made it conceivable for us to connect whenever we consider it necessary. Working from home by giving online courses and lectures, holding meetings via Zoom and many other digital platforms, and staying in touch with our families using video calls would have been impossible without it. In addition, to online shopping, doctor consulting and promotions also happen in this digital space now.

However, do not be blindsided; it is not all sweetness and light. Living in a virtual society comes with many risks and threats; in addition, as the digital world grows every day, people need to be educated about the potential risks of the internet. To prevent these threats, everyone in society, including the country's Government, should be aware of cybersecurity. When digitalisation was increased globally to a higher level cyber-attacks also increased proportionately . Cybercriminals use danced tools and tactics to gain access to compromise the network, disrupt operations, financial gain, steal credentials and information.

The common definition of Cybersecurity can be stated as "a discipline that covers a way to defend devices and services from electronic attacks by depraved actors like hackers, script kiddies, spammers, cybercriminals and insiders". Most of today's professionals focus a lot on determining the best way to defend all assets, from computers and smartphones to networks and databases, from attacks. Forbes 2022 lists out numerous terrifying cyber security challenges, everything from supply chain disruption to increased smart device risk to a continued cyber security talent drought. As reported by Cybercrime Magazine, cybercrime will cost the world $10.5 trillion yearly by 2025. Moreover, worldwide cybercrime costs are anticipated to ascend by nearly 15 per cent yearly throughout the following four years. Nowadays cybersecurity is an economic and national security crisis.

In the Sri Lankan context, increasing cybersecurity is a must. To illustrate this several cyber-attacks that happened in the past few years. The LTTE has hacked the Government's websites several times. The Easter Sunday attack created a new dimension to cyber threats. The Islamic State of Iraq and Syria (ISIS) used social media platforms to disseminate propaganda mainly through social media to Sri Lankans. Moreover, ISIS used social media sites, particularly Facebook to spread hate speech online to provoke anti-Muslim violence. Considering these facts, cybercrimes have gone beyond boundaries, and a country like Sri Lanka should follow a stringent policy for enhancing cyber security.

According to the National Cyber Security Index (NCSI), it is a global index that measures the preparedness of countries to prevent cyber threats and manage their cyber events. As per the ranking of the NCSI, Sri Lanka has advanced to the 69th position (the year 2021) from the 98th position (the year 2020) out of 160 countries. However, according to the NCIS's 2022 ranking, Sri Lanka holds the 78th position. That's a drawback when compared to 2021. What could have caused this to happen?

When analysing the reasons behind these cyber-attacks, even though the Government gives their full contribution to protecting valuable information they have, most the Government institutions' websites security with less concern for adapting protective security measures was noted, as well as usage of simple and obvious passwords. In recent years, Sri Lanka's greater dependence on critical infrastructure, industrial automation, and cyber-based control systems has resulted in a growing unforeseen vulnerability to a cyber security threat. Protecting and assuring the availability of critical infrastructure is vital to both the Sri Lankan and South Asian economies. It is therefore crucial that cybersecurity professionals address the issue.

Even more important cyber security and data protection becomes more urgent with the onset of e-Government services in Sri Lanka. The hazard of fraud and identity theft increases, in conjunction with the risk of cyber-attacks. As a result of this Sri Lankan Government has initiated the "Personal Data Protection" bill which is an appreciable milestone to protect data privacy.

Adding to this, to diminish these cyberattacks, reinforcing an effective cybersecurity strategy is of utmost importance to Sri Lanka. Implementing awareness programs for both Government and private sector officials will be an effective thing to develop their cyber security knowledge. Also, building separate cybersecurity forces in the Government sector is another effective initiative to reduce the risk of cyberattacks and uplift their knowledge. Furthermore, these awareness programs should be implemented at the university, schools, and community levels. Singapore has displayed cybersecurity notices for the public even in the lifts and public places and also provides continuous awareness for the community. In Sri Lanka, Government and private institutions can engage with each other and develop a productive strategy to increase the cybersecurity system in Sri Lanka.

Apart from these strategies, there are many things that can implement. Such as printing cyber safety posters for distribution, displaying cyber safety messages on digital screens, developing TV advertisements about cybersecurity, developing a number of cybersecurity awareness video clips for publishing on social media, etc. Another essential point is that there is a lack of human resource facilities available in Sri Lanka in the cybersecurity field. It may cause to leave

cybersecurity professionals to leave the country. That's why there should be continuous improvement in this field. In view of the above, we live in a connected world, therefore, everyone in the society has an individual role to play in cybersecurity.

Cybersecurity cannot be looked at from a theoretical angle; it has to be looked at from a practical perspective. If we are facing countrywide cyber-attacks? How do we deal with minimum numbers of human capital? Except for these things, there are many other ways to stringent cyber security in the country. In addition to the above, it will recommend considering below key areas ensuring cybersecurity and resiliency within the country,

Develop and implement a national strategy/ roadmap for e-Government on digital transformation.

Contribution to global cyber security;

- – Collaborate with a professional association of cybersecurity specialists in other countries
- – Collaborate with other Governments/ exchange programs, public-private partnership
- – Design and implement controls for the Protection of digital services, data, information, and critical infrastructure.
- – Design and implement the national-level cyber security operation/ command center.
- – Implement a Cybercrime unit and Digital forensics unit at the national level

When closely looking at Sri Lanka's cyber security, it can be understood that there are direct threats to the country's political, economic, social, and technological spheres. It also poses absolute threats to the country's legislation, as it all requires new legislation relevant to the Sri Lankan context to be prepared for the country to face new challenges. Nowadays, since the daily routine of people is mostly revolved around the internet, especially this work from home, distance learning has become an essential thing, and with the competition that has aroused from the advancements in the technological field, it is a vital need to be apprehensive on security measures which will help to protect the Sri Lankan society as a whole.

About the Author:

Thusitha Bulathgama is a Research Assistant at the Institute of National Security Studies (INSS), the premier think tank on National Security established under the Ministry of Defence. The opinion expressed is his own and not necessarily reflective of the institute.

By Thusitha Bulathgama