Speech of Hon. Minister Deepak Balgobin
"National Cybersecurity Strategy Seminar 2020" - Pearle Beach Resort, Flic en Flac – 3rd March 2020 at 09.30am

Mrs M. J. S. Valere, The Permanent Secretary of my Ministry

Mr. Maurice Campbell, Project Leader, Cyber Resilience for Development Project (Cyber4D)

Mr. Hannes Krause, Country Coordinator – Mauritius, Cyber Resilience for Development Project (Cyber4D)

Mrs Joanne Esymot, Executive Director of the National Computer Board,

Delegates from the Cyber4D Project,

Heads of Ministries and Departments,

Heads of Parastatal and Private Organizations,

Distinguished guests,

Members of the Press,

Ladies and Gentlemen,

Good Morning and welcome to the Cybersecurity Strategy Seminar, an initiative of my ministry and the Cyber Resilience for Development (Cyber4D) Project.

First of all, I wish to express my gratitude to all delegates who have travelled from Europe to Mauritius for this event. I am pleased to be amongst you all today to address you on this occasion.

I am proud to say that Mauritius has been chosen for the project as part of East Africa. The role of Mauritius in this programme is to be a model cyber resilient country and share its experience and best practices with other countries in the region. I understand that the project has started in May 2018 and will be running till 2021.

Ladies and Gentlemen,

I could gather that the objective of the programme is to increase the cyber resilience of countries through "raising awareness on cyber threats; developing national cyber security strategies; providing for information assurance and resilience; setting up, training and equipping Computer Emergency Response Teams, building early warning, information sharing and analysis capabilities as well as protecting Critical Information Infrastructures.

Ladies and Gentlemen,

The growth of the Internet has brought with it a consequent rise in the number of cybercrimes. With all the great and productive things about the Internet, there is a limitation - anyone using it, is exposed to its associated security risks which can have adverse consequences. Some of the more widespread examples of the criminal activity include scamming, denial of service attacks, computer viruses, phishing, email spying and hacking.

As stated by IBM, 68% of global organisations claim that they are not equipped and able to handle a complex cyber-attack. It is noted that more cyber-attacks, hacks, and data breaches are motivated by financial purposes than anything else.

According to Verizon in 2019, 71 percent of cyber-attacks are motivated by money; most of these attacks are perpetrated by people outside of the organizations, with the majority being carried out by organized criminal groups.

In this context, it is not viable to expect that defenses can prevent all cybercrimes. However, we are not defenseless targets. There are numerous things we can do to deter cyber criminals who are constantly looking forward to stealing our information and destroy our data.

Dear participants,

At this point, allow me to remind you that Mauritius was the first country to have adopted a very comprehensive Data Protection Act, aligned with the principles of the EU General Data Protection Regulations.

Organizations should keep on developing capabilities for detecting incidents when they arise, minimizing the impact on business and critical infrastructure, and tying these capabilities together in a comprehensive framework.

Information security today is a rapidly evolving game of advanced skill and strategy. Thus, the security models of the past decade are no longer useful. Today’s information security leaders acknowledge that playing the game at a higher level is required to achieve effective security. They know that the very survival of their business relies on their understanding of cyberthreats, preparing for them, and responding to them in a timely manner.

Ladies and Gentlemen,

One of our Government's main objective is to shape the right environment to make the Internet more accessible and secure to the citizens of Mauritius. My ministry, through CERTMU and IT Security Unit is working hard to enhance the Internet development by devising appropriate strategies and policies to provide a secure environment for one and all.

Ladies and Gentlemen,

The broadband Internet penetration in Mauritius is currently more than 90 percent and this compares very favorably with the 31 percent of internet penetration that exist in Africa according to the World Bank. This accessibility to the Internet has played a significant role in the island's reform and opening up efforts and helped to build and strengthen the connections between Mauritius and the rest of the globe.

We truly believe that while development is the ultimate goal, security is the guarantee of achieving that goal. Mauritius has always placed great emphasis on cybersecurity. Without a secure environment, we know that development will be deprived. Therefore, we are trying our best to ensure that Mauritius remains prepared for the challenges that comes on our way.

Ladies and Gentlemen,

I strongly believe in order to achieve a resilient and secure environment, national cyber strategies play an important role for a country. Please let me elaborate that my ministry has developed and implemented two strategies to keep itself prepared to combat cyber threats. One is the National Cybersecurity Strategy and the other one is the National Cybercrime Strategy.

Cybersecurity strategy provides an overview of what it takes to effectively protect information systems and networks and gives an insight into the Government's approach and strategy for protection of cyberspace in the country, whereas the cybercrime strategy sets out the Government's approach to fight cybercrime through improved law enforcement capability, effective criminal justice framework and active international engagement.

Through these strategies number of projects have taken shape, some of them have been completed and some are in progress. The areas covered through these strategies include measures such as setting up of a centralised cyber incident reporting system known as Mauritian Cybercrime Online Reporting System (MAUCORS), development of national cyber incident response plan, development of CIIP Policy, setting up of a Cyber Defence Centre and ITU Centre of Excellence, adoption of ISO 27001 standard, ratification of AU Convention on Cybersecurity and Personal Data Protection, child online protection capacity building, review of Computer Misuse and Cybercrime Act in line with the Budapest Convention on Cybercrime and with the AU Convention on Cybersecurity and Personal Data Protection etc.

On international collaboration, Mauritius is already the party to the Commonwealth Cyber Declaration signed by the Prime Minister in April 2018 in London on the occasion of the holding of Commonwealth Heads of Government Meeting. Mauritius has also an MoU with the Government of Estonia in the field of Information and Communication Technology which was signed in November 2017.

These initiatives have played an important role in the ranking of Mauritius in the Global Cybersecurity Index of the ITU and has placed the country 1st in Africa since the past 6 years. I recognise this as a great achievement and it has been possible by the hard work put in by my ministry and the support of the Government led by the right Honourable Pravind Jagunath, our Prime Minister.

In view of consolidating our position as a safe and secure IT destination, my Ministry will shortly operationalise a Security Operation Centre (SOC) in our Government Online Centre (GOC). The SOC will analyse incoming and outgoing connections at the GOC in order to preemptively identify and respond to cyberthreats.

Ladies and Gentlemen,

Please now allow me to say few words on the very important event of today i.e. cybersecurity strategy seminar. It is organised by the Cyber4D team as part of their effort to assist Mauritius in building cyber capacity in different areas of cybersecurity. This event will last for two complete days, today and tomorrow and will help to discuss and identify the gaps of our existing cybersecurity and cybercrime strategies and propose the best practices based on the Estonian experience.

Since we are in the stage of reviewing the national Cybersecurity Strategy for Mauritius, this exercise has been planned on a very ripe moment and will be instrumental in formulating a comprehensive National Cybersecurity Strategy. I commend this initiative of Cyber4D along with other activities which have been organised since May 2018. I understand this is the 12th activity.

I believe this is an opportunity for us to engage with Cyber4D experts to discuss in length on the different aspects of strategy formulation and use it as an ingredient into the forthcoming national cybersecurity strategy development.

Ladies and Gentlemen,

Before I conclude, I would like to thank the Cyber4D team and everyone who contributed to this seminar. I shall now end my speech, I thank you for your attention and presence. I wish this seminar all the success it deserves. I wish you all fruitful deliberations and thank you for your attention.

I now declare the **National Cybersecurity Strategy Seminar** officially open.