# Speech of Honourable Deepak Balgobin

## Minister of Information Technology, Communication and Innovation

# Cybersecurity wakeup call for Directors, CEOs and key Decision Makers by Rogers Capital

**Hennessy Park Hotel, Ebène**

*8th February 2022*

- **Ms Sandrine Valere, Permanent Secretary of my Ministry**
- **Mr. Dev Hurkoo, Managing Director, Rogers Capital Technology**
- **Heads of Ministries and Departments**
- **Dear participants**
- **Members of the Press**
- **Ladies and Gentlemen**

A very good morning to you all.

I wish to express my thanks to Rogers Capital for gracing us with such a capital event. And I am told that presentations on cybersecurity which follow will really be captivating.

The world is calling for an innovation of products and services we consume, through the process of digitalisation. There are many reasons for the need to digitalise. First of all, by automating business processes through digitalisation, there is a gain in efficiency, which allows for optimised usage and redeployment of the scarce resources being employed.

Secondly, the adoption of digital solutions gives rise to new products and new lines of businesses for a more flourishing economy. Next, the digitalisation of services prolongs business and social activities in periods of crisis as witnessed during the pandemic.

**Ladies and Gentlemen,**

Today, new and emerging technologies have completely reshaped the face of the business world. Artificial Intelligence, Blockchain, Virtual Reality, Internet of Things, Internet of Everything, Robotic Process Automation and 5G have become the new buzzwords.

As technology progresses, unfortunately cyber threats also evolve in the dark, in parallel. Some people would do anything to compromise the success of technology-enabled solutions. It could be for money, for personal pleasure, or for tarnishing the reputation of others. Cyber criminals are using the same evolving technology to create and disseminate information which is not based on facts or which is totally fake.

Cybercriminals are becoming more and more sophisticated and are perfecting their methodologies in the quest to attack critical information infrastructure. In 2017, the world saw massive cyber-attacks by the WannaCry Ransomware encrypting data on critical systems and claiming ransom payments in crypto-currency. More recently, in 2021, the Colonial Pipeline Company was subject to a ransomware cyberattack causing it to shutdown the operations of its pipeline system in the US for five days, which resulted in a temporary fuel shortage.

The Computer Emergency Response Team of Mauritius, CERT-MU, which falls under the aegis of my Ministry, has prepared a Critical Information Infrastructure Protection Policy. The objective is to determine and identify critical systems and accordingly recommend the mobilisation of resources to counter the effects of possible attacks on those targets.

The statistics gathered for the last four years, through the Mauritian Cybercrime Online Reporting System (MAUCORS) are alarming. Cases reported in 2021 are around 5 times more than those in 2018. In 2021, 2320 cases have been reported as compared to 426 cases in 2018. For the month of January this year, the MAUCORS has recorded 208 cases.

**Ladies and Gentlemen,**

At a time when we are facing unprecedented threats from rogue hackers and all sorts of cybercriminals, this Government has unveiled a new piece of legislation to take urgent actions, to give the Government and the private sector the tools we need to combat cyber threats and to protect each and every citizen of our country.

The Cybersecurity and Cybercrime Act was passed in Parliament in November last and this new piece of legislation that I have introduced provides for a modern framework aligned with the Budapest Convention on cybercrime.

The Act also makes provision for the setting up of a National Cybersecurity Committee which will look after matters relating to cybersecurity and cybercrime, and promote capacity building on the prevention, detection and mitigation of cyber threats, amongst others.

**Ladies and Gentlemen,**

My Ministry is in the process of finalising the National Cybersecurity Strategy 2022-2024. The Strategy will provide for enhanced measures to mitigate cyberthreats and the effects of cyber-attacks. It will take on board the necessary measures to push the security of our cyber environment to new heights.

We are also exploring the porting of our Security Operations Centre (SOC) on emerging technologies for faster response to cyber threats. The proposed SOC

will monitor network traffic on the Government Online Centre (GOC) which is the Data Centre of Government as well as other Government infrastructures, and defend those assets against potential cyber-attacks around the clock and in real time.

Furthermore, Mauritius has been participating in the EU Cyber4D (*Cyber Resilience for Development*) activities since 2018. Cyber4D is a European Union initiative which promotes cyber-resilience and cybersecurity in order to protect public and private enterprises throughout the world. CERT-MU has been acting as the coordinating body for Cyber4D programmes. Such activities have enabled us to constantly assess and consolidate the preparedness of Mauritius to detect cyber threats before the attacks actually occur and to promptly respond to major cyber-attacks.

I wish also to highlight here that Mauritius is ranked 1st in the Africa region and 17th globally in the 2020 edition of the ITU Global Cybersecurity Index. We must reckon that our efforts will never be enough as our enemies are capable of deploying endless tricks to annoy us.

**Ladies and Gentlemen,**

Today cyber-attacks have gone beyond what could have been imagined and security safeguards for businesses are costing a substantial amount of the budgets allocate for their whole information systems. Sometimes businesses may not even be aware of their being subject to a cyber attack or other security issues.

This workshop will unveil the means that our enemies exploit to compromise our business activities. It will be a unique opportunity for us decision makers to take cognizance of such dangers and understand the possible measures that

could be taken to mitigate their associated risks. If you aren't aware of those dangers, you won’t be able to get out of the mess they create.

**Dear Friends,**

This wake-up call event comes at the right time to boost the relentless efforts Government is already making to react against such misdeeds. It also demonstrates a strong business-friendly relation between the Public and the Private sector. The more so that it fits very well with the celebration of the Safer Internet Day today.

Before I conclude I would like to thank Rogers Capital once more for its endeavour to equip the island with the necessary resources to reinforce the protection of its ICT landscape.

I wish all participants fruitful deliberations and thank you all for your attention.