Speech of Hon. Deepak Balgobin
Minister of Information Technology, Communication and Innovation

Workshop on Cybersecurity
State Informatics Limited

8th May 2023 at 10 00hrs
Caudan Arts Centre

- **Mr Abhishake Jugoo, Chairman of the State Informatics Limited,**
- **Mr Kemraz Mohee, CEO of the SIL,**
- **Mr Kaleem Usmani, Officer in Charge of the CERT-MU,**
- **Representatives from the Public and Private sector Organisations,**
- **Dear participants,**
- **Ladies and Gentlemen,**

Good Morning to you all.

I am honoured to be addressing you today. It is a fact that one of the most pressing issues of our time is Cybersecurity. We are all aware that we face constant and evolving threats from malicious persons who seek to exploit our digital vulnerabilities and undermine our security, privacy, and prosperity.

The impact of cyber-attacks can be devastating, causing damage to businesses, public sector organisations, and individuals alike. High-profile cyber-attacks have caused significant damage to businesses and public sector organisations, highlighting the importance of robust cybersecurity measures.

We cannot afford to be complacent or reactive when it comes to cybersecurity.

Instead, we must be proactive, vigilant, and strategic in our approach. Cybersecurity is everyone's responsibility. Individuals, businesses, and public sector organizations must take it seriously and implement appropriate measures to protect data and networks.

Ladies and Gentlemen,

My ministry has launched numerous digital projects with the objective of providing secure access to government services and facilitating information sharing.

These initiatives include MauPass, Mokloud, and Mausign digital certificate.

We have focused on using digital technology to enhance the quality-of-service delivery to the public. In addition to these projects, the government has also announced large-scale national initiatives such as eHealth for the Ministry of Health & Quality of Life and Automated Fingerprint Identification System (AFIS) for the Mauritius Police Force.

These projects will transform the way healthcare and public safety services are delivered in our country and will depend heavily on secure and robust digital infrastructure.

It is of utmost importance that we make cybersecurity a top national priority and a strategic imperative.

Ensuring the security of these digital transformation projects and protecting all associated data is critical. We must remain alert and vigilant in guaranteeing the security of our digital infrastructure to uphold the public's trust in these digital services.

Cyber incidents could come with great uncertainty and complexity. There have been more than 1200 online attacks cases reported to the Mauritian Cybercrime Online Reporting System (MAUCORS) from January 2023 to date. This concerns Hacking, Online Harassment, Identity Theft, Scams and Frauds, the list is long and the perpetrators and their motivations are often obscure.

The Government is working together with regulatory bodies to develop fresh legislation and policies that would enforce stringent cybersecurity frameworks on organizations in both the public and private sectors.

The new Cybersecurity and Cybercrime Act was voted in 2021 with a view to modernize our legal framework in order to ensure that the Mauritian legislation remains strong and resilient to cybercrime.

In addition, we are investing in our cyber capabilities, including personnel, technology, and infrastructure, to ensure that we have the necessary resources to detect and respond to cyber threats effectively.

We are also continuously strengthening our cyber defences by implementing robust security measures to prevent cyberattacks and minimize the damage caused by any attacks.

Furthermore, enhancing our cyber resilience is essential to minimize the impact of cyberattacks and ensure that we can recover quickly from any disruptions. This is achieved through regular testing of our cyber defences, conducting cyber drills by the CERT-MU team, and developing incident response plans that outline clear procedures for addressing cyber incidents.

Moreover, we need to foster a culture of cyber awareness and responsibility among all stakeholders, from public officials to private sector partners to individual users.

This means educating ourselves and our employees about the latest cybersecurity threats and best practices, implementing security protocols that are appropriate for our organization's needs, and being proactive in monitoring and responding to potential security breaches.

Ladies and Gentlemen,

Cybersecurity is not just a national concern. It is a global challenge that affects every country.

Therefore, promoting international cooperation in the cyberspace is critical.

We are working closely with other countries to share information, coordinate responses to cyber-attacks, and hold accountable those who violate international norms.

We are also supporting innovation and research in cybersecurity, and the development of skills and talents of our cyber workforce.

This means investing in training and education programs that will help us build a pipeline of skilled cybersecurity professionals.

CERT-MU has since long been organising cybersecurity trainings in Mauritius to empower our citizens as well as our working population on various aspects of cybersecurity. In order to extend training to international participants CERT-MU is, since February this year, an ITU Academy Training Centre in the field of Cybersecurity.

Ladies and Gentlemen,

We must work together to build a resilient and secure digital environment for all. In this context, I commend this initiative of State Informatics Limited in organising this workshop on Leveraging on a strong Cybersecurity Framework for Risk Reduction and Compliance.

I would like to acknowledge the presence of high calibre speakers in this workshop and in particular the delegates from the Andhra Pradesh Technology Services who are responsible to run the Security Operations Centre (SOC) of the State of Andhra Pradesh.

I wish you all a fruitful deliberation, and I have the privilege to declare the Workshop open.

Thank you.