Speech of the Hon. Deepak Balgobin

Minister of Information Technology, Communication & Innovation

Cyber Resilience and Simulation Workshop – CERTMU

20th April 2023

Shri Atal Bihari Vajpayee Tower, Ebène

- **Mrs. Sandrine Valere-Bolli, Permanent Secretary of my Ministry,**
- **Dr. Viv Padayachi, Chairman of the National Cybersecurity Committee,**
- **Dr Kaleem Usmani, Officer-in-Charge of CERT-MU,**
- **Heads of Departments & Parastatal Organisations,**
- **Ladies and Gentlemen,**
- **All protocol observered**

Good Morning to you all.

I am delighted to be here this morning hosting this important event on Cyber Resilience and Simulation organised by the Computer Emergency Team of Mauritius (CERT-MU), a department falling under my Ministry.

Cybersecurity is a must-have !

To protect our citizens, our societies and our economy.

And so, the Government is devoting a lot of time and energy on how we can improve our overall resilience in the face of future challenges.

It is therefore imperative that we enhance our collective efforts and I am confident that this workshop will provide yet another contribution towards that direction.

You will have an insight in the new Cybersecurity and Cybercrime Act 2021 whereby different sections of this law will be elaborated for your better understanding.

In addition, there will be a panel discussion with experts from the public and private sector who will enlighten you on the opportunites and obstacles of Cyber resilience.

I am also informed that a mini exhibition has also been organised to showcase the security products and solutions by the local companies.

This is done with an objective for the participants to know what are the lastest solutions and services available in the market.

You are all welcomed to visit the stands.

Ladies and Gentlemen,

Cyber security and resilience is essential to all organisations operating in the digital economy. As digital services become more interconnected, the increasing sophistication and frequency of cyber-attacks has the potential to cause widespread damage.

A cyber incident may cause significant harm to consumers, destabilise markets and affect trust and confidence in a country's digital system.

In today's modern age, as warfare goes online, we are more likely to witness cyber-attacks through the use of state-of-the-art technology.

Cyber incidents could come with great uncertainty and complexity.

Hacking, Online Harassment, Identity Theft, Scams and Frauds, the list is lon and the perpetrators and their motivations are often obscure. 1162. This number represents all the online attacks recorded on the Mauritian Cybercrime Online Reporting System (MAUCORS) from January 2023 to date.

The high Internet penetration rate among our citizens and the adoption of social networks as well as the ease of downloading and viewing contents online are all contributing in making our cyber space more exposed to attacks.

Therefore, to best protect a Government’s or a company’s assets, there needs to be a continual evolution to be more resilient in order to drive key outcomes.

Consequently, we need to adopt cyber resilience in order to continuously and intelligently move forward, despite adverse cyber events.

With the advent of 5G and proliferation of the Internet of Things (IOT), the need to continuously adapt will accelerate further in a hyper-connected world.

The focus for cyber resilience has to be able to evolve and match this increasing pace of change to ensure the Government and businesses are operating securely for the citizens.

Ladies and Gentlemen

My Ministry has taken bold and serious actions to protect the Mauritian Cyberspace.

Legal Framework

In December 2021, I presented in our parliament a new Cybersecurity and Cybercrime legislation, the Cybersecurity and Cybercrime Act 2021, with a view to modernize our legal framework in order to ensure that the Mauritian legislation remains strong and resilient to cybercrime.

National Cybersecurity Committee

We have also constituted a National Cybersecurity Committee in this new piece of legislation which will have as prime objective to advise the Governement and implement Government policy on matters related to Cybersecurity and Cybercrime.

I am sure that the chairperson of the National Cybersecurity Committee, Dr Padayachi will enlighten you further on the role of this particular committee in the presentation which is scheduled later during the day.

Capacity Building

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.

The Centre will directly contribute to build knowledge and skills among professionals in the ICT.

It will be actively engaging the region as well as different parts of the world for cyber capacity building.

The first training will be scheduled in June this year.

Incident Reporting and Resoultion

The MAUCORS platform is helping organisations and population in general to report their cyber incidents. This centralised reporting system has alieviated the hassles that our citizens were having to report any cybercrime issue. The system is doing the facilitation to resolve issues and I urge critical organisations to report their incidents for a timely resolution.

National Cyber Incident Response Plan

Moreover, the Government has also approved a National Cyber Incident Response Plan to manage cyber crisis situations. Currently the National Cybersecurity Committee is working along with CERT-MU to check its effectiveness.

Technical Infrastructure

The Security Operations Centre (SOC) set up at the level of the Government Online Centre is being strengthened by my Ministry to enable better monitoring of the threats in the government infrastructure.

In September last year, Mauritius launched a national cyber threat intelligence sharing platform which is known as MAUSHIELD. This new platform will be integrated with the SOC to better analyse and check the cyber threats.

Policies and Strategies

Currently, my Minsitry is working on the implementation of the Critical Information Infrastrucutre Framework that will allow to strengthen the security of the Mauritian Critical Information Infrastrcutres.

The National Cybersecurity Committee has been tasked to look into the implementation of the framework and I understand that the Committee has already started their work towards achieving that goal.

International Cooperation

CERT-MU in collaboration with the AfricaCERT and SADC has been organising international cyber drills. The countries in Africa have benefitted from these excercises. Last year, CERT-MU has led the organisation of Africa Cyber Drill and the SADC simulation excercise. Currently, CERT-MU is in the process of working with Malawi CERT for the organisation of their simulation exercise.

We have been helping Rwanda, Togo, Botswana, Malawi and Seychelles in different areas of cybersecurity.

Ladies and Gentleman,

These initiatives have played an important role in the ranking of Mauritius in the ITU Global Cybersecurity Index and has placed Mauritius FIRST in Africa since the past 8 years and is ranked 17th globally.

My ministry is working hard towards improving the global ranking of Mauritius in the next edition of the ITU index which is due by the end of this year.

With these words Ladies and Gentlemen, I now have the pleasure to declare the workshop on Cyber Resilience open and I wish you all a fruitful deliberation.