

Speech of Honourable Deepak Balgobin  
Minister of Information Technology,  
Communication and Innovation

Sophos Indian Ocean Partner Roadshow 2022  
&  
Lithe Solutions Distributor Ltd

Thursday, 8<sup>th</sup> December 2022 at 18hrs  
Maison de l'Etoile, Eureka, Moka

- **Honourable Sunil Bholah, Minister of Industrial Development, SMEs and Cooperatives,**
- **Mr Ameer Kamani, Director Business Development – Lithe SD**
- **Mr Viral Shah, Sophos,**
- **Captains of the ICT sector from Mauritius, Madagascar and Seychelles,**
- **Ladies and Gentlemen,**

Good evening to you all.

I am delighted to join you for this Roadshow and I want to congratulate the whole team of Sophos and Lithe Solutions Distributor Ltd for bringing together professionals from the cybersecurity community in Mauritius and the region.

This event is an important platform to recognise individuals and organisations for their significant contributions to improving our cybersecurity.

I must say that such initiatives from the private sector to better protect the Mauritian cyberspace is laudable. We all know that cybersecurity is a united approach and has to be dealt together, which will eventually promote Public and Private Partnership.

## **Ladies and Gentlemen,**

The cyberthreat landscape is dynamic and will keep on changing thus exposing digital world to numerous risks. As much as great inventions and technologies empower us, their conscious misuse can also lead to unprecedented damage and pose real threats.

Technical failures and malicious attacks occur at alarming and ever increasing intervals. Inadequate response to these incidents result in consumers losing confidence, businesses losing money and even national security being put at stake.

Whatever the motivation and whoever the attacker, they are all far too common and their consequences are far too costly. Costs can run into the millions and leads to a reputational damage. The number and impact of cyber incidents continue to grow.

We have to cooperate better and more efficiently than ever before.

It is evident: vulnerabilities, backdoors and incidents need to be detected and acted upon as early as possible. Many companies suffer from cyber-attacks without knowing that they are being victims of it.

Statistics are truly alarming !

From January to date, we have recorded more than 2600 cybercrimes occurring on social media platforms on the Mauritian Cybercrime Online Reporting System (MAUCORS) which is managed by our Computer Emergency Response Team – Mauritius (CERTMU).

There were 2815 incidents reported last year and 1890 in 2020.

These incidents concern Hacking, Online Harassment, Offensive Contents, Identity Theft, Cyber Bullying, Cyber Stalking, Scam, Frauds, Phishing and Malware.

Each minute somewhere around the world a cyber-attack is happening. Now, literally this very second, someone's computer is being hacked, someone's personal records, financial information, or intellectual property is being stolen and sold on the black market.

Someone is losing money as a result of that attack. This 'someone' could be me, you, or your bank, university or Government.

In addition to a rise in the frequency of attacks, the attack vectors employed by cybercriminals are also changing. The cyberthreat landscape has taken completely different dimension during the COVID-19 era.

According to the experts, cloud security and artificial intelligence (AI) is an area that require greater focus, ransomware attacks are becoming more sophisticated and challenging. Experts also estimated that technological advances such as 5G and the widespread use of IOT devices will bring numerous threats.

**Ladies and Gentlemen,**

Let me now briefly elaborate on some of the initiatives taken by our Government to combat these cyberthreats. The Mauritius Government, along with the regional and international partners, is very much committed to address the issue of cybersecurity and cybercrime.

It is worth noting that cybercrime is not only a question of attacks against the confidentiality, integrity and availability of computer data and systems but against the core values and the human development potential of societies increasingly relying on information technology.

In this view, we have the obligation to protect our society and individuals against such cybercrimes. To this effect, an efficient criminal justice response is needed. It also requires effective international cooperation given the transnational nature of cybercrime.

My Ministry has come up with a new law on cybersecurity and cybercrime to ensure that legal framework of Mauritius remains strong and resilient to cybercrime. The Cybersecurity and Cybercrime Act was enacted in December 2021. Currently, it is being promulgated.

This modern law is also aligned with the Budapest Convention on Cyber Crime and the African Union Convention on Cyber Security and Personal Data Protection to deal with the transnational threats.

I would like to point out that my Ministry is in the stage of finalising the new Cybersecurity Strategy to cater for the evolution and sophistication of cyber threats due to the expansion of internet connectivity and proliferation of connected devices, including 5G technology which Mauritius has embraced recently.

**Ladies and Gentlemen,**

In September 2022, my Ministry launched an online platform for sharing cyber threat intelligence in a real-time and in a secure and confidential manner. The platform is named MAUSHIELD and it will help public and private sector organisations to improve their cyber defense capability and stay ahead of emerging trends and cyber threats.

MAUSHIELD allows cyber threat information sharing through a Membership Programme opened to Public sector organisations, Critical sectors, Private sector organisations, Small and Medium Enterprises, Academia, Non-profit organisations and Individuals.

I also take this opportunity to invite interested parties to apply for the Maushield membership, which is free of charge and take advantage of the numerous benefits from this newly set up system.

National Cybersecurity Committee

Another matter of great concern for the Government is the protection of critical information infrastructure which provides essential services to citizens.

To address this issue, currently, the National Cybersecurity Committee set up under my Ministry is working towards implementing the Critical Information Infrastructure Policy. The implementation of this Policy will help critical sectors to keep their IT infrastructures secure and resilient.

### **Ladies and Gentlemen**

Today's event represent one of the initiatives where Mauritius is engaged in promoting regional collaboration. In addition, Mauritius is assisting other regional countries to strengthen and improve their cyber resilience. As part of this initiative, Mauritius is helping regional agencies to conduct cyber simulation exercises.

With regards to international collaboration, Mauritius is actively involved in the discussions of the UN Open Ended Working Group and Ad Hoc Committee, an initiative of the United Nations to bring all member states on a common platform to discuss how to respond to cyber threats effectively.

### **Ladies and Gentlemen,**

Please allow me to conclude on one of the ultimate requirement to prevent cyber-attacks. Yes I am talking about capacity building. Today, there is a shortage of cybersecurity manpower around the world including Mauritius.



Qualified professionals are in great demand as governments and businesses pay more attention to cyber risks. This demand will only increase as the frequency and consequences of cyber threats continue to grow.

In this endeavor, Mauritius has been engaging within the region to provide capacity building through the ITU centre of Excellence. So far more than 800 professionals have been trained from some 35 countries through this centre.

Mauritius will continue to provide capacity in this area.

I would like to thank Sophos and Lithe Solutions Distributor Ltd and all those who contributed to make this event happen.

To everyone present today, thank you for leading the way in growing, developing and advancing our cybersecurity ecosystem.

It is our collective mission, that is, the entire cybersecurity community, to protect and to strengthen it.

Before ending, I wish to seize this opportunity to wish you and your family a Merry Christmas and a Happy New Year 2023.

**Thank you!**