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

"Compliance, Governance & Risk Management around the Cyber Risks and Threats in our ecosystem" by Harel Mallac Technologies

Thursday, 5th May 2022
Hennessy Park Hotel, Ebène

- **Mr Antoine Harel, Chairman, Harel Mallac Group,**
- **Ms Sandrine Valere, Permanent Secretary of my Ministry,**
- **Mr Shateeaum Sewpaul, General Manager, Harel Mallac Technologies,**
- **Mrs Namita Jagarnath Hardowar, President, Mauritius Chamber of Commerce and Industry,**
- **Dear Speakers and Participants of this symposium,**
- **Members of the Press,**
- **Ladies and Gentlemen,**

Good morning to you all.

Intro

1. First and foremost, let me thank Harel Mallac Technologies for hosting this event to tackle a priority topic which is cyber risks and threats in our ecosystem.
2. Cybersecurity is a pertinent and pressing issue confronting any Government or organisation, be it in the public or private sector.
3. Cyberspace should primarily be a peaceful domain.
4. Government needs to act, and we are.
5. But in tackling cybersecurity, one cannot work alone.
6. Given how cyber threats are borderless, constantly changing and increasing in sophistication, collaboration and harnessing the collective ideas and wisdom of likeminded experts, are key to enhancing Cybersecurity.
7. It is increasingly difficult to outsmart the attackers, and as defenders, we have to unite our strengths, expertise and resources, to create necessary eco-system and synergy with a view to countering threats and attacks.

Ladies and Gentlemen,

8. The world over has seen a rise in digital threats and malicious cyber activities, and more particularly in the African countries.
9. These include sabotaged public infrastructure, losses from digital fraud and illicit financial flows, and national security breaches involving espionage and intelligence theft, amongst others.
10. According to the American software company Proofpoint, 88% of organizations worldwide experienced spear phishing attempts in 2019.
11. Risk Based Security American company specialized in vulnerability intelligence, breach data and risk ratings, published statistics showing that data breaches exposed 36 billion records in the first half of 2020.
12. ID Theft Resource Center, an American non-profit organisation, has recorded 11,762 system breaches between January 1, 2005, and May 31, 2020.
13. In the United States, the Colonial Pipeline, a major fuel company fell victim to a ransomware attack this year, which led to its entire fuel distribution pipeline being shut down, causing shortages across the US East Coast and influencing oil prices globally.
14. On the regional front, due to the growth of digital transformation across Africa, the continent has become an attractive target for cyber criminals.
15. Cyberattacks cost Africa 3.5 billion US Dollar in 2019, according to Serianu, a Kenyan based security firm.
16. More specifically, Nigeria recorded a total of 650 million US Dollars in losses.
17. Also, Kenya incurred losses of 210 million US Dollars, and Tanzania had losses of 99 million US Dollars.
18. These incidents have raised awareness of the importance of protecting systems against cyber-attacks.

19. Addressing these vulnerabilities requires an ever-greater commitment to cybersecurity.
20. It is now the opportune time for Governments to take full advantage of the digital revolution to empower our citizens and enhance transparency in both the public and private sectors.
21. This will not happen until data is stored in safe and trusted systems that protect privacy and are difficult for criminals to breach.

Ladies and Gentlemen,

22. Cybercrime is not only a question of attacks against the confidentiality, integrity and availability of computer data and systems but it is also an attack against the core values and the human development potential of societies which are increasingly relying on information technology.
23. It is therefore our duty to protect our society and individuals against such cybercrimes. To achieve our goal, we need an efficient criminal justice system.
24. As cyberthreats are rising, so should Government's actions to counter them.
25. The **Cybersecurity and Cybercrime Act of 2021**, strives to ensure that the Mauritian cyberspace remains strong and resilient to cybercrime.
26. The Act englobes the provisions of the Budapest Convention on Cybercrime and the Malabo Convention on Cybersecurity and Personal Data Protection. In this endeavour, my Ministry sought the assistance of the **Council of Europe**.
27. The law also takes on board the recent technological developments, norms and standards, and put in place a forward-looking regulatory framework that addresses the challenges of today's world.

28. In addition, measures are being taken to continuously consolidate our readiness in the face of the ever changing and increasing cyberthreats. Likewise, the CERT-MU (Computer Emergency Response Team), operating under my Ministry, has been conducting online training programmes under the ITU Centre of Excellence label as well as holding cyber drills.

29. The National Cyber Incident Response Plan has been formulated to set out the steps to be followed should the country be in the midst of a cyber crisis. The next logical step would be for us to simulate a major cyber incident and test the National Cyber Incident Response Plan.

30. This is the task that I intend to give to CERTMU to drive in the coming weeks.

Ladies and Gentlemen,

31. Reporting cases of cyberbullying, cyberextortion, sextortion, phishing and many others need to be an easy process so that victims may swiftly alert the authorities for action. With this is mind, CERTMU and my Ministry have set up the MAUCORS (Mauritian Online Cybercrime Reporting System) platform.

32. Personal data protection is also very important and subject to a lot of cyberthreats. Recognising the need to have a very robust framework, Mauritius adopted a revamped Data Protection Act in 2017 which is, aligned with EU's General Data Protection Regulations (GDPR).

Ladies and Gentlemen,

33. Now is the time for us to take even more bold steps in cybersecurity to make sure that we are prepared, resilient and capable of responding to potential online aggressors.

34. I congratulate our private sector partners for having strengthened your cyber defences by implementing the best practices developed over the last years.

35. Today's event organised by Harel Mallac Technologies is testimony of the drive by the private sector to further enhance our eco-system and to work in close collaboration with public & private stakeholders to better position Mauritius on the international cyberspace.

36. I commend Harel Mallac Technologies for setting up such a distinguished panel which will surely contribute in the continuous effort by all parties from Mauritius and overseas to deliberate constructively on today's subject matter which remains high on the agenda of the Government.

37. On this note, I wish you a fruitful and productive interactions.

Thank you for your attention.