Financial Services Commission

Speech of the Chief Executive

Seminar on "Cybersecurity Wake-up Call" – Hennessy Park Hotel, Ebene

06 July 2022

The Honourable Mahen Kumar SEERUTTUN, Minister of Financial Services and Good Governance,

Mr Samade Jhummun, Chief Executive Officer of Mauritius Finance

Mr Dev Hurkoo, Managing Director, Rogers Capital Technology

Representatives of the Industry

Delegates and participants

Distinguished Guests,

Ladies and Gentlemen,

All protocols observed.

Good morning to you all,

First, please allow me to thank the organisers for inviting me to this event to say a few words on this particularly important theme of "Cybersecurity".

During the pandemic, the world has experienced unprecedented cybercrimes in the forms of phishing attacks, identity theft, insider frauds, sextortion, fake medicine and ransomware attacks. According to statistics from the website "techradar.com", the total cost of cyber

incidents when added to the cost of putting security measures in place, was estimated at 1 trillion US Dollars in 2020, that is 1% of the world GDP.

In 2021, a Bank for International Settlements report titled "Covid-19 and cyber risk in the financial sector" highlighted that the financial sector has been hit by hackers relatively more often than other sectors during COVID-19 in 2020. By all means, cybersecurity is now more essential than ever.

Ladies and Gentlemen

The reputation of an International Financial Centre is also measured by its ability to put in place adequate systems, procedures and laws to effectively fight cyber criminality. Today, our IFC is at a critical juncture in its continued pursuit of establishing Mauritius as a hub for emerging technologies. Mauritius is among the first countries in the Eastern and Southern African region which is in the process of adopting comprehensive legislation on virtual assets and initial token offerings. Our financial services sector is undergoing transformational changes through the adoption of disruptive technologies, particularly in the FinTech area. These rapid advances in financial technology are transforming the economic and financial landscape, offering wide-ranging opportunities.

However, as financial services' dependency on technology increases, so does the impact of a disruption, whether accidental or intentional by threat actors. From my experience in the electronic payment business, I am very conscious that even minor cyber security incidents could easily undermine trust and derail such innovations.

Dear Audience

According to a publication from the IMF entitled "The Global Cyber Threat" published in 2021, the assessment that a major cyberattack poses a threat to financial stability is axiomatic— not a question of *if*, but *when*.

In February 2020, Christine Lagarde, president of the European Central Bank and former head of the IMF, warned that a cyberattack could trigger a serious financial crisis. In April 2020, the Financial Stability Board (FSB) warned that "a major cyber incident, if not properly contained, could lead to broader financial stability implications." The potential economic costs of such events can be immense and the damage to public trust and confidence significant.

In this time of transformation, technology-enabled business models change the sources and nature of financial stability risks. The concerns are even more worrying when we know that the frequency, scale, and complexity of cyber-attacks are constantly increasing, day-by-day.

Ladies and Gentlemen,

Addressing cybersecurity is not a one-off exercise but rather a continuous process where the cyber-risk awareness culture is placed at the centre. Cyber-risk awareness should pervade every aspect of an organization – its people, its processes and its technology. In 2019, the FSC issued a Circular Letter on Cyber Risk Security Governance, with the objective of recommending board-level oversight over the risk governance function, particularly relating to cyber security practices. As you might expect, we see licensees taking a number of different strategies to compliance – there is no one right answer, but we do have some expectations in this area that I want to share.

I can summarise these by saying we expect 'a security culture', driven from the top down, that is, from the Board, to senior management, down to every employee. Cybersecurity culture is key to getting a greater return on technological resources and strengthening the weakest security link – which is you – "people". Further, the perception that cybersecurity is only the responsibility of the IT department is taking a myopic view of the problem.

Executive figures should emphasise that cybersecurity is everyone's responsibility by highlighting security for what it is – a structure that facilitates an organisation's business vision and mission, a means of ensuring business continuity and ultimately, a positive investment. We are looking for licensees to have good governance around cyber security in their organisation – by this I mean senior management engagement and responsibility.

The FSC is working on updated guidelines to give the industry a greater focus on cyber resilience, as well as to provide further guidance on new technologies and emerging cyber threats. The objective would be to help strengthen our financial sector's resilience to cyber risk, through better cyber hygiene.

Let me highlight some key initiatives undertaken at the level of the FSC.

First, I recently took the initiative of setting up a Joint committee between the FSC and Mauritius Finance to act as a springboard between the Regulator and the Industry on cyber security matters. Interesting ideas and potential projects have emanated, amongst which is the organisation of today's event. The committee is also empowered to provide consultative advice and feedback in respect of new cyber security guidelines that the FSC shall introduce.

Further to that, the FSC is currently exploring the area of digital Identity and digital signatures, for the purpose of both facilitating business process and, **more importantly, improving trust and security** in the financial services business. I further wish to inform that the FSC will shortly implement ISO:27001 – Information Security Governance Framework.

Second, the FSC is building its capacity to perform Digital Forensics. As the world's financial systems advance in digital technology and cryptocurrency, we have seen an

unprecedented rise in cyber-enabled financial crimes. These crimes no longer take months of in-depth planning, but can now be committed within minutes because of the processing power of computers and the speed of the internet. Crimes such as embezzlement, money laundering insider trading become more complex to detect.

The FSC is addressing this challenge by turning it into an opportunity to build up its Digital Forensics skillsets and capabilities. We expect the importance of digital forensics in fighting financial crime to grow significantly in the coming years.

Ladies and Gentlemen,
Going forward, given the growing complexity of cyber-attacks and how interconnected the global financial system is, close cooperation is essential to ensure the cyber resilience of our financial sector. To that effect, the FSC will be looking into areas of co-operation with leading regulators, in view to enhancing our cyber security capabilities.

In furtherance, our staff continue to work to enhance FSC's cyber security posture, while supporting our digital transformation initiative. We are aligned with the Government's efforts to improve the nation's cybersecurity. We are vigilant to the evolving threat landscape and continuously maintain the highest level of resilience. This focus cannot be compromised. Although the monetary cost of improving cyber resilience may seem high, the costs of successful attacks – in terms of both financial damage and reputational impact – are far higher. In addition, we continue to evaluate our data footprint and improve our data collection processes so that we collect only the data we need to fulfill our mission.

Dear Audience,
I also seize this opportunity and I have been reporting this in a number of fora that as part of our awareness campaign on VAITOS, service providers dealing with virtual assets need to apply for relevant activity licence. I therefore also make an appeal to the public not to deal with people or institutions without a licence.

Ladies and Gentlemen,

Cybersecurity is a matter of common interest for one and all. We as regulator and you as industry players need to work hand in hand to achieve a secure financial system in Mauritius.

With these words, ladies and gentlemen, I would like to wish you a very fruitful deliberation ahead and thank you for your kind attention.

Dhanesswurnath Thakoor
06 July 2022