Transcript of Speech delivered by Mr Tan Kiat How,
Senior Minister of State,
Ministry of Communications and Information,
at Tata Communications WeConnect (17 Feb 2023)

Mr Lakshmi, MD & CEO Tata Communications
Distinguished Guests,
Ladies and Gentlemen

1. Good afternoon, everyone. It is my pleasure to be here at Tata Communications WeConnect 2023.

2. The Tata Group has a long partnership with Singapore dating back to the early 1970s. Since then, the company has expanded, employing close to a million employees worldwide today. As part of the Tata Group, Tata Communications has been an enabler of the wider digital ecosystem, with enterprise solutions spanning cloud, IoT, cybersecurity and more. These solutions are important in helping businesses transform and capture new opportunities, especially in a post-pandemic world.

3. At the same time, digitalisation brings with it threats and challenges that consumers, businesses and governments must work together to address, in order to preserve trust in the digital ecosystem. Let me highlight two such challenges today. The first is on ransomware attacks, and the second is on online scams.

4. Ransomware attacks have intensified in scale and impact around the world, evolving from a sporadic risk affecting a small number of systems to a large-scale systemic risk that can disrupt critical infrastructure and essential services, and threaten national security. A case in point was the ransomware attack on the Colonial Pipeline in 2021, which shut down the largest fuel pipeline in the East Coast of the United States, affecting fuel supply to 50 million consumers.

5. Closer to home in Singapore, 137 ransomware cases were reported to the Cyber Security Agency of Singapore (or CSA) in 2021. This was a 54 percent increase from 2020. The cases affected mostly SMEs from sectors such as manufacturing and IT. And there might be more cases that go unreported. For example, the US FBI shared last month that only 20 percent of US ransomware victims step forward to report such cyber incidents.

6. Online scams are also becoming increasingly prevalent. Just last week, the Singapore Police Force (SPF) shared that there were around 7,100 phishing scams last year, a 41 percent spike from 2021. A staggering S$51 million was lost to phishing scams in Singapore in the last two years alone. With scammers constantly evolving their tactics, it is a perennial challenge for us to instil public awareness and take preventive measures.

7. These statistics are a grim reminder that we must work together to address such threats promptly, to ensure that our people and our businesses trust the digital ecosystem.

8. So how can we build trust? Let me highlight three ways in which we are doing so in Singapore.

9. First, we must put in place effective regulations to enhance the security and resilience of our digital infrastructure and protect users in the online space.

10. In 2018, we passed the Cybersecurity Act, which gives us a legal framework to protect Critical Information Infrastructure (or CII) which deliver essential services, such as water and power.

With the evolving cyber threat landscape, CSA is reviewing the Act to see if the scope of CII needs to be expanded, and whether to include other digital infrastructure and services.

11. Just last November, we passed the Online Safety Bill to minimise users' exposure to harmful digital content, and equip them with tools to protect themselves online. Designated Social Media Services will need to comply with a Code of Practice for Online Safety, which we expect to implement in the second half of this year. So that is the first area – effective regulations, and we are adapting it and making sure it is relevant for the times.

12. Second, we will continue to invest in research and innovation, in areas such as AI, cybersecurity and trust technologies. This will be crucial in growing our capabilities and anchoring Singapore as a Trusted Digital Innovation Hub.

13. Since 2020, we have started six trust-related research programmes across NTU, NUS, and SMU. These include how privacy tech can be applied to social media and machine learning, the role of law and ethics in technology, the use of blockchain in finance, and more.

14. Last year, we launched the Digital Trust Centre, which will lead Singapore's R&D efforts in trust technologies, and support talent development in this space.

15. Thirdly, we must enhance the cybersecurity and data protection capabilities of our companies: Last year, we launched the Cyber Trust and Cyber Essentials marks to recognise companies that have put in place good cybersecurity practices and measures to address their cybersecurity risks. These certifications will provide greater assurance to firms and consumers alike, fostering greater trust in the digital economy.

16. We are also refreshing our Industry Digital Plans (IDPs) to incorporate a roadmap on Cybersecurity and Data Protection measures. This will help companies identify and adopt suitable tools and practices to safeguard their systems. For some of you who may not be aware of what these IDPs are, every sector and every industry is digitalising rapidly, and the Singapore government is working together with the different government agencies and industry partners in these sectors to develop customised digital plans for each sector. An SME in the manufacturing sector will be very different from an SME in logistics, healthcare, or finance. So we are working sector by sector, developing industry digital plans for that sector, curating services, products, solutions that are relevant for the digital needs of those sectors for not just companies, but their employees and workers, with industry digital plans across the board supporting the broad based digitalisation of our economy.

17. I have spoken about what we are doing in Singapore to preserve trust in our digital economy. It is crucial that we work with like-minded countries to advocate for a global digital framework that is interoperable, resilient, and secure – this will facilitate cross-border innovation and trust in emerging technologies and applications, and build confidence among our citizens to transact digitally across borders. I like the term that Mr Lakshmi used – hyperconnected ecosystems. And Singapore wants to be part of this hyperconnected ecosystem globally.

18. For this reason, we have been pursuing Digital Economy Agreements (DEAs) with like-minded partners, which align digital rules and standards.

19. Within Asia, we led the development of the ASEAN Model Contractual Clauses. These are contractual terms which facilitates cross-border transfer of data across the region. We also have the APEC Cross Border Privacy Rules, or CBPR, which help to bridge differing privacy laws in APEC, and reduce barriers to data flows. We are now working with partners to promote the CBPR system globally.

20. In the last two years, we have also formalised mutual recognition of our Cybersecurity Labelling Scheme with Finland and Germany covering various consumer Internet of Things (or IoT) devices. This scheme will allow IoT device manufacturers to stand out from competitors and facilitate access to new markets.

21. In conclusion, to realise the potential of digital transformation, it is critical to address threats, and build trust in the digital ecosystem. Singapore will continue to do so through effective regulation, investments in research and innovation, and building the capabilities of our enterprises. We will also contribute towards a global ecosystem of trust through international partnerships.

22. Today, at Tata Communications WeConnect, we have captains of industry gathered here together, to explore solutions that can help businesses build trust, catalyse change, and accelerate growth. I hope this event will build on our shared efforts in creating a trusted digital ecosystem for our citizens and businesses to thrive in.

23. I wish all of you a fruitful discussion.

24. Thank you.