Ministry of Communications and Information
An Engaged and Connected Singapore

[FOR IMMEDIATE REPORTING]

Opening Address by Mrs Josephine Teo, Minister for Communications and Information at the ISTARI Charter Asia-Pacific Cyber Congress (20 Mar 2024)

Professor Tan Eng Chye, NUS President

Ms Akvile Giniotiene

Mr Robert Hannigan

Distinguished Guests

Ladies & Gentlemen

1. Thank you for inviting me to speak to you today.

2. Later this year, the world will descend upon Paris for one of the biggest highlights in sports, the quadrennial Olympic Games. Well before any ticket is sold, any athlete arrives at the village, or any fan sets foot in a stadium, Interpol has warned that the biggest security threat this Olympics will be cybercrime.

3. After all, the Tokyo Olympics of 2021 was reported to have encountered 450 million cyber-attacks, more than twice as many as during the 2012 London Olympics. These attacks can disrupt any activity that needs IT systems support, and that includes ticketing, games administration, transportation, broadcasting… you name it.

4. By now, cybersecurity has become a global imperative. In every aspect of our lives where there is a digital dimension, there will also be concerns about cyber risks. Likewise in Singapore, where digital developments are relatively advanced, we have learnt to value cybersecurity and to prioritise the development of strong capabilities.

5. We are committed to strengthening the security and resilience of our systems. We also appreciate platforms that allow us to participate in global discourse, so we can learn from colleagues and also contribute our experience.

6. This is why we host the Singapore International Cyber Week each year – which many of you are familiar with – and are active at multilateral platforms for cybersecurity like the United Nations Open Ended Working Group.

7. We participate actively in plurilateral efforts like the Counter Ransomware Initiative, and champion regional initiatives such as the establishment of an ASEAN CERT in Singapore.

8. We are therefore happy that ISTARI chose Singapore to host its pan-ASIAN ISTARI Charter Event, to bring together regional thought leaders in cyber.

9. However, even as we do our part to advance global conversations on cybersecurity, we are acutely aware that our contribution builds on efforts at home.

10. In my speech therefore, I will discuss how we are continuing to work hard on our cybersecurity in three areas:

i. First, the legislative foundation to ensure security and resilience;

ii. Second, the cybersecurity posture of our organisations and companies; and

iii. Third, the development of cybersecurity talent and the growth of our industry.

<u>The Government is looking at how to strengthen the cybersecurity and resilience of today's digital infrastructure</u>

11. In Parliament earlier this month, I said that the Cybersecurity Act will be updated to look beyond critical information infrastructure that it already covers today, and seek to cover other systems and entities.

a. The expanded coverage will include foundational digital infrastructure, such as cloud services and data centres, that so much of our economy and society now relies on.

b. The amendments will ensure that appropriate cybersecurity measures are put in place, given the importance of this infrastructure.

12. I also announced that the Ministry of Communications and Information (MCI) is studying the introduction of a new Digital Infrastructure Act (DIA).

a. This is because when systems are disrupted, the reasons are not always because of weak cybersecurity measures.

b. Rather, they can be due to vulnerabilities in the broader security arrangements, such as something as basic as exposure to weather elements. Or it could be the lack of resilience built into the digital systems that make recovery efforts long-drawn and unwieldy.

13. The DIA therefore complements the Cybersecurity Act to give assurance to our people and businesses that digital services are trustworthy and reliable.

a. As part of this effort, we will be studying similar legislative efforts around the world, such as those from the EU and Germany.

b. We will implement these regulatory measures with other efforts, such as providing guidance and best practices to digital infrastructure and service providers.

14. Consistent with past efforts, we have consulted widely on these new legislations. Many of you in the room have provided your useful inputs, and we are grateful for them.

<u>More can be done to raise cybersecurity posture of Singapore companies and organisations</u>

15. Beyond digital infrastructure, the cybersecurity and resilience of our companies are also important. They provide the services that people use, and define our online experiences.

16. To establish the baseline of the current status and guide our efforts, the Cybersecurity Agency of Singapore recently completed a survey of the cyber health of organisations here.

17. More than 2,000 organisations were covered, across 23 industry sectors and 7 charity sectors. The majority of them have encountered at least one cyber incident, such as ransomware or social engineering attempts at phishing, in the year prior to being surveyed. They are therefore informed respondents.

18. The findings will be released next week but let me share some of the insights with you in advance.

19. First, the survey asked about the specific measures that these organisations adopted in 5 categories, such as using secure configuration settings for hardware and software, controlling access to data and services, and updating software on devices and systems. In each of the 5 categories, on average, organisations adopted about 70% of the essential measures. This is reasonably encouraging.

20. However, CSA believes that partial adoption of essential measures is inadequate. As the saying goes, we are only as strong as the weakest link. Unless all these essential measures are adopted, the organisations are still exposed to unnecessary cyber risks.

21. In CSA's view, the "passing mark" should be set high enough to give assurance – to your C-suite, to employees, to suppliers and to customers. That means adopting the full package of essential measures in all of the 5 categories. In this regard, there is much room for improvement as only one-third of the organisations surveyed adopted all the measures in at least 3 categories.

22. SMEs fared better in some categories compared to others. For example, we found high (>70%) adoption of the full package of essential measures relating to software updates and incident responses. But SMEs are exceptionally weak in virus and malware protection, and access control, where full-package adoption is well below 20%.

23. [NEW] According to the survey, almost 60% of both businesses and non-profits reported a lack of knowledge or experience to implement cybersecurity effectively. In some ways, this is not at all surprising. Cyber risks have increased and continue to evolve quickly. This has contributed to the shortfall in cyber professionals; even the most sophisticated organisations struggle to keep up.

24. It was reassuring therefore, that 75% of organisations surveyed were at least aware of the need for cybersecurity and how to get help. We hope the survey findings help to motivate organisations to take the next step, from awareness to implementing concrete actions to minimally "pass" by adopting all the essential cyber measures.

25. CSA is committed to providing stronger support to these organisations. For example, we developed the Chief Information Security Officer (CISO)-as-a-service scheme, which engages cybersecurity consultants to develop tailored cybersecurity health plans for those in need. This helps to plug the access gap.

26. For the cybersecurity industry and service providers, these survey findings also highlight opportunities where you can step up and step in. After all, protecting the cybersecurity of our organisations and digital infrastructure is a team effort. Government efforts matter but they will not be enough. We will need to work with the cybersecurity ecosystem – that is our industry and academia – to build and sustain our efforts.

Singapore is supporting the development of talent and the growth of our industry

27. Given the importance of a strong ecosystem, we launched the CyberSG Talent, Innovation, and Growth Plan – also known as the TIG Plan. This is a comprehensive approach to boost Singapore's cybersecurity talent and industry development efforts.

28. As part of this plan, the NUS CyberSG TIG Centre has been set up to promote collaborations between cybersecurity stakeholders from academia, government, international organisations and industry partners like ISTARI.

29. Let me now provide some updates on our TIG efforts.

Talent Development

30. Talent is a critical success factor for any ecosystem, and so the TIG Plan seeks to nurture all cybersecurity professionals, whether they are students interested in embarking on this career, or senior leaders already at the apex of their organisation.

31. To support students aspiring to be entrepreneurs, ISTARI will provide internship and mentorship opportunities to students participating in the **NUS Overseas College's** entrepreneurial education programme. I trust that this will be the start of a meaningful relationship between ISTARI and the TIG Centre here in Singapore.

32. **[Announcement]** At the management level, CSA, Singapore Management University, and ISTARI will be collaborating on the third run of the **Cybersecurity Strategic Leadership Programme (CSLP)** to equip current and future generations of local cybersecurity leaders with a deep level of understanding on global key drivers that shape cybersecurity strategies.

33. CSA has conducted two iterations of the Programme over the span of two years, with 46 C-suite participants successfully completing the program. It is often the case that the leaders at the top must be equipped with knowledge and understanding to ask the right questions of the people that they have assigned important tasks to - and CSLP is intended to do just that. So, participants at the C-suite levels are exposed to a whole range of cybersecurity issues that their staff grapple with, but which they themselves may only have a shallow understanding of at the initial stage. Therefore, the idea of the programme is to deepen their understanding. The programme has received good feedback. In fact, every participant in the last cohort has said that they would recommend the program to their peers. The Programme is now open for applications, and I encourage interested leaders to apply.

Industry Growth

34. Moving on to industry growth, I will touch on two areas in particular: catalysing the development of innovative solutions and creating opportunities for businesses beyond Singapore.

35. **[Announcement]** To develop cutting edge solutions, I am pleased to share that, with help from the TIG Centre, CSA will be expanding its **Cybersecurity Call for Innovation;** also known as **CyberCall**. This programme will be offered twice this year, not only once, so we will make two innovation calls. This is part of our redoubling of efforts to stay ahead of emerging challenges.

a. One example of useful innovations from previous CyberCalls is the product named "Asset Based Cyber Defence", "A-B-C-D" in short. It is a collaborative effort between three companies – SecureAge, InsiderSecurity and ReaQta that aims to provide SMEs with an automated end-to-end cybersecurity solution covering multiple attack vectors. Currently, there are already more than 300 customers who are trying out the product.

36. If you have novel cybersecurity challenges or solutions, I encourage you to throw your hat in the ring when applications open.

37. The TIG Plan also facilitates the export of Singapore’s cybersecurity products and services, as we believe that our useful products can benefit not just the Singapore market, but the world. Therefore, we support local companies seeking to expand their business abroad, and one of the ways we are doing this is through overseas mission trips to explore opportunities together.

38. **[Announcement]** The TIG Centre will be leading a delegation of Singapore cybersecurity companies to London this June to understand common cybersecurity problems to be solved, to forge connections and to broaden their business reach. Businesses keen on exploring opportunities to enter the UK, or other foreign markets, should keep an eye out for applications opening in the coming weeks.

Conclusion

39. In conclusion, building and sustaining trust in our digital domain requires a whole-of-ecosystem effort.

40. The Government does not expect to do this alone. Instead, we welcome partnerships with colleagues in industry and academia.

41. We believe that by working together as a team and thinking creatively, we can raise the level of trust and resilience in Singapore’s cybersecurity. Thank you.

-End-