Ministry of Communications and Information
An Engaged and Connected Singapore

# OPENING SPEECH BY MRS JOSEPHINE TEO, MINISTER FOR COMMUNICATIONS AND INFORMATION, AT THE CYBERSECURITY AWARDS 2022 ON 11 NOVEMBER 2022, 7.20PM

Mr Johnny Kho, President, AiSP,

Colleagues and Friends

## Introduction

1. Good evening. I am delighted to join you on this occasion, and I want to congratulate the whole team at AiSP for being able to bring together the cybersecurity community again for the awards and gala dinner.

2. It goes without saying that this evening is an important occasion. This event is an important platform to recognise individuals and organisations for their significant contributions to improving our cybersecurity in Singapore.

3. My heartiest congratulations to all our award recipients. Let me also express my appreciation to AiSP and the associations from the Singapore Cyber Security Inter Association (SCSIA) for organising this event.

4. Now everyone in this room is keenly aware of the growing sophistication of cyber threats, and the speed of their evolution.

5. I spoke to you at the last Cybersecurity Awards about Log4j. Since then, unfortunately, there have been more incidents. In April 2022, a ransomware attack on Costa Rica crippled essential services in the country, forcing the Costa Rican government to declare a state of national emergency.

6. In February 2022, a cyber-attack, in relation to the activities in the war in Ukraine, hit at the satellite communications provider Viasat and caused network disruptions across neighbouring countries in Europe.

7. We know with the continued proliferation of network technologies such as Cloud and IoT, our attack surface will only continue to expand.

8. These threats may seem far away from us, but we in this room will remember that distance is no barrier to cyber criminals.

9. What this means is that we cannot afford to be lacking in vigilance, to be letting down our guard and we must constantly remind ourselves that it is really not a question of if, but when.

10. From that perspective, you are all under immense pressure. There are tremendous demands being placed on anyone that owns or has to operate a system with cyber risks. You are constantly working to help secure the systems and making sure that they remain protected.

11. So, the question for us is that what makes for a healthy and vibrant cybersecurity ecosystem in Singapore? From MCI's, as well as CSA's, perspective, there are

really three things. One is talent. The second is teamwork and the third is trust. I will share some updates on what the Government is doing on each of those fronts.

**Key Message 1: We need to build a strong pipeline of cyber talent to keep up with the challenges of securing our cyberspace.**

12. First, let me talk about talent because that is the number one item on everyone's agenda. Each time we meet with the community, you will always impress upon us how important it is for us to build up the talent pool in Singapore for cybersecurity. That is because people are at the heart of everything we do in cybersecurity – they are behind all our cybersecurity technologies, systems, and processes.

13. This is why each year at the Cybersecurity Awards, we celebrate the individuals and organisations who have not just excelled in their own domains, but also contributed to developing and nurturing others in the industry.

14. The challenge of securing our growing cyberspace calls for a larger and more skilled cybersecurity workforce.

15. In Singapore, there is still a demand-supply gap even though the number of cybersecurity professionals has more than doubled **from 4,000 in 2016 to about 11,000 today**.

16. This is also why the Cyber Security Agency (CSA) launched the SG Cyber Talent Development Fund earlier this year, to support the engagement, development and advancement of the cybersecurity workforce.

17. What are we doing under this fund? Under this Fund, CSA is providing support to individuals, communities and associations through three types of projects:

    (i) Community projects to engage and grow the cybersecurity community, raising people's awareness of the opportunities that are available to them;

    (ii) Skills development and recognition projects to develop or recognise cybersecurity skillsets; and

    (iii) Training and Job Placement projects that are more novel or untested, but which offer some potential for us to grow the cybersecurity community. All three types of projects are important, and they each bring something different to our ecosystem.

18. We have supported several exciting projects through the Fund.

19. For example, to attract and develop female professionals to the cybersecurity industry, we supported the SheLeadsTech Conversion Programme.

20. What does it do? The programme kicked-off in April this year with a modest first batch of 11 participants but it aims to provide female professionals who were not in an IT environment but are willing to make a career switch into Governance, Risk and Compliance (GRC) roles in the cybersecurity industry. In other words, they have adjacent skills that can be brought to bear, and to benefit the cybersecurity industry.

21. CSA will continue to support initiatives, like this, to develop and grow the local cybersecurity talent pipeline. If you've always wanted to try out an idea to promote the development of our cybersecurity workforce but never knew where to start, you are very welcome to tap on this fund.

22. At the same time, we continue to welcome global cybersecurity talent from around the world, who contribute to the development of Singapore's cybersecurity sector.

**Key Message 2: Cyber defenders need to work as a team to combat cyber threats.**

23. The next factor that is critical for success is teamwork. We all know that no single individual, organisation or government can secure our cyberspace on its own.

24. This year's Cybersecurity Awards includes a good mix of winners – from individuals to organisations, from students to the most respected leaders of the profession, from SMEs to very large MNCs and from vendors to end-users.

25. This reflects the diversity of our community. Each of us deals with different cybersecurity challenges in our respective roles. And each of us also recognises it is only through working together as a team – across industry, academia, and government – that we can more effectively combat cyber threats.

26. The Government is certainly committed to working with you and to encourage teamwork and partnerships across the public and private sectors. One example is the annual Cybersecurity Industry Call for Innovation (CyberCall).

27. It brings end users together with cybersecurity companies, including start-ups to jointly identify cybersecurity challenges specific to Singapore's needs and develop solutions for these challenges.

28. Since CyberCall started in 2018, we have supported 22 cybersecurity companies to develop over 30 of such solutions, and I look forward to seeing even more exciting collaborations and innovations emerging out of this initiative.

**Key Message 3: The cybersecurity ecosystem needs to safeguard trust in the cyberspace.**

29. The final, and I think most critical factor for success is trust. With so much of our lives now reliant on digital technologies, it is absolutely critical for the public to trust that our digital infrastructure works the way it is intended to. You come into any building, you do not expect it to collapse on you. You do not go into any mall and expect fires to break out. You have come to expect a level of safety and yet this level of safety is not experienced to the same degree in the cyber domain, whether you are an individual or a business.

30. So, if people do not feel safe transacting online, how is it that they can continue to do so on an extended basis? Can they feel confident that the information they share online will not inadvertently be leaked and misused by threat actors? That must change the way you see your digital transactions. So, trust, undergirding all our other efforts, including talent and teamwork, must not be eroded. And, so we have to work doubly hard to uphold this trust and to prevent it from being diminished.

31. It is our collective mission – it is something that we share, the mission of the entire cybersecurity community – to protect that trust and strengthen it. We therefore need to continue to safeguard our systems and networks, and ensure they are resilient to cyber threats.

32. Certainly, on the part of the Government, we will continue to  nurture and protect this trust, but we cannot do it alone. We are very cognisant of that. Individuals and enterprises also have a key role to play.

33. This is why CSA has rolled out a series of cybersecurity toolkits. These toolkits help enterprise leaders, SME owners and employees learn about their specific roles and the measures they can take to keep their companies safe from cyber threats.

34. Another example is the cybersecurity certification scheme for companies, comprising the Cyber Essentials and Cyber Trust marks.

35. This was launched by CSA earlier this year to certify companies that have met certain cybersecurity standards. These trust marks allow businesses to differentiate themselves, giving their clients and partners the confidence to work with them.

36. I encourage business leaders and cybersecurity professionals present here today to tap on these resources..

## Conclusion

37. As we approach the end of yet another eventful year, I am glad that we have this opportunity to gather and to celebrate the achievements of our cybersecurity colleagues.

38. To everyone present today, thank you for leading the way in growing, developing and advancing our cybersecurity ecosystem. I have a feeling that when we gather in a matter of three years, five years, ten years, the cybersecurity community will be one that has grown in both breadth and depth. I see this happening because digitalisation is not stopping. Digitalisation will continue to be a mainstay of our economic development. Whether or not there are economic downturns, it is a trend that is not going to stop in any way. So, this community has every reason to be hopeful about the future, to be optimistic about the prospects, and also every reason to be confident that you can be a leader.

39. Thank you very much for inviting me.

.

*****************************