Ministry of Communications and Information
An Engaged and Connected Singapore

OPENING SPEECH BY MRS JOSEPHINE TEO
MINISTER FOR COMMUNICATIONS AND INFORMATION
AT THE 4TH CYBERSECURITY AWARDS CEREMONY ON 14 JANUARY 2022

Mr Johnny Kho, President, AiSP
Colleagues and Friends

1. I am happy to join you this evening to honour outstanding contributions to the cybersecurity ecosystem both in Singapore as well as to the region.

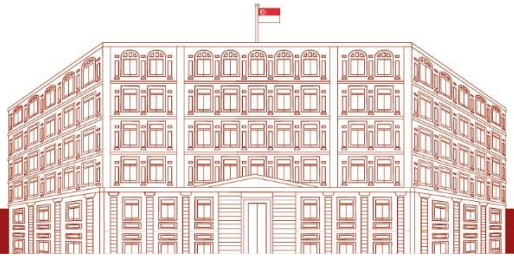
2. I want to thank AiSP, and the other associations from the Singapore Cyber Security Inter Association, for putting this event together.

3. Your collective effort is precisely the kind of unity and teamwork that we must harness to meet the cyber threats confronting Singapore.

4. These cyber threats are serious and urgent**.** We need to get this message out to everyone else. We want to highlight the kind of examples that they should be paying attention to. You take for example the critical vulnerabilities surrounding Log4J. They allow hackers to potentially take full control of affected systems.

5. Log4J's presence in countless applications and products - and even supply chains - means that organisations have real trouble knowing just how exposed and at risk they are.

6. How does one tackle problems when we don't even know they exist? Or if you believe they exist in the system, but do not know where they are?



7. And yet slowness to act can be very costly. There are numerous examples, I will just point out a few. Because of Log4J a cryptocurrency trading platform had data belonging to nearly two million customers stolen by hackers, because it did not manage to patch its vulnerable server in time. Meanwhile, cyber threat actors of all stripes have wasted no time in exploiting this vast attack surface. Within a couple of days since the first vulnerability's disclosure, malicious attempts to exploit it surged 300 times! Probably more by now. Hackers are constantly devising new methods of exploitation, so more attacks are likely to be forthcoming.

8. I shall not attempt to calculate the number of man-hours that the Log4J episode has cost. It is safe to say that just about every IT team, in Singapore and around the world, has been working tirelessly since December to study developments, share information, implement patches and respond to Log4J-related incidents.

9. My colleagues at CSA, too, have been in the trenches with you. During the festive season in December, CSA has issued more than 20 Log4J-related alerts and advisories. CSA also conducted a briefing on the attack vectors and mitigations for cybersecurity practitioners. Despite being held in the last week of December, the briefing was well-received by the community. It attracted more than 300 attendees, including cybersecurity chiefs from the CII sectors.

10. All of this demonstrates the tremendous amount of resources and commitment by all stakeholders across the cybersecurity ecosystem, in managing the fallout of Log4J -- a single open-source component. Consider the fact that the average application today includes over 500 open-source components. More vulnerabilities will surface, perhaps more severe ones.

11. We also have to contend with the increasing sophistication of both state-sponsored hackers and cybercriminal groups. High-profile incidents over the past year, from SolarWinds to the Colonial Pipeline and the Kaseya incident, have shown how disruptive supply chain breaches and ransomware attacks can be. We are now acutely aware that the effects of cyber-attacks can spill over to the physical world. Whether it is the shutdown of big supermarket chains or the disruption of healthcare services, the impact is tangible.

12. So while we must try our best to prevent breaches, we must also recognise that cyber-attacks are not a question of “if”, but “when”.

13. Some attacks will eventually succeed, so our cybersecurity posture must account for this. How can we do that? First, by adopting an “assume breach” mindset. Take it that a breach may have already occurred in your system. Step up monitoring for unusual activity and suspicious connections in your networks. Continuously verify and validate all activity in your systems.

14. Second, by improving our cyber resilience. If threats are present, we must deal with them decisively. If an attack succeeds, we must recover swiftly. The goal is to minimise any disruption to business operations, especially the delivery of essential services.

15. Third, by enhancing the people, processes and technologies undergirding our cybersecurity posture. We must continue to cultivate a sufficiently large and skilled cybersecurity workforce. We must continue to develop more advanced capabilities within and among the existing practitioners We must continue to practice and review our processes pertaining to crisis response and recovery. This is so that when a cyber-attack hits, the entire ecosystem can react as a well-oiled machine. And can bounce back quickly.

16. To that end, CSA will hold the fourth edition of Exercise Cyber Star during the last week of January, just before Chinese New Year. Together with all 11 CII sector leads and their CII owners, we will test their response to complex attack scenarios and improve where there are gaps.

17. The constant shifts and curveballs in the cyber landscape mean we need to adjust and synergise our efforts. That is why we launched an updated Singapore Cybersecurity Strategy in 2021. The Strategy is not merely a government blueprint, but a call to action for all stakeholders in our cybersecurity ecosystem, including the associations and companies represented here tonight. I saw how many of you have heeded the call during the recent Log4J fallout, and I am confident that you will continue to contribute actively.

18. The Government is in it with everyone for the long haul. Today, I am pleased to announce CSA's launch of the SG Cyber Talent Development Fund. This will be a boost to our efforts to grow cyber talent pipeline. The Fund will support communities and organisations in coming up with initiatives that will help our cybersecurity ecosystem grow. If you have ideas for expanding or enriching the cybersecurity community, for developing and recognising skills, or for creating more training and job placements, we want to hear from you.

19. I want to end my remarks by addressing all the finalists. Thank you for the work that you have done for our cybersecurity ecosystem. I look forward to more innovation and excellence. Your efforts will certainly inspire the next wave of cybersecurity leaders.

20. The fact that we have cybersecurity is not a given, but through commitment and capabilities, we can surmount the many challenges and seize opportunities ahead. Thank you.