Ministry of Communications and Information
An Engaged and Connected Singapore

OPENING REMARKS BY MR TAN KIAT HOW, SENIOR MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION, AT CISO SINGAPORE ON 22 AUGUST 2023, 9.50AM

Distinguished guests

Ladies and gentlemen

Introduction

1. Good morning. I am happy to be here at CISO Singapore 2023.

2. I thank Corinium Group for organising this event and bringing together such a distinguished group of cybersecurity leaders from across Singapore and Asia, to exchange views on trending cybersecurity issues such as cloud security and supply chain risks.

Urgency to adapt to recent changes in the threat landscape

3. Recent developments have transformed our cyber threat landscape, and we need to adapt quickly to these changes. Let me touch on a few examples.

4. First, the rise in adoption of emerging technologies like AI by malicious actors, especially generative AI, has resulted in increased sophistication of cyberattacks, and at scale. For instance, publicly-available AI software like ChatGPT has been shown to be able to support the rapid development of cyber exploits, and AI can be used to develop malware payloads with dynamic signatures, at scale.

5. Second, our digital ecosystem is also becoming more interconnected, which means that a cyberattack and disruption of one organisation's systems can easily affect another's.

a. For instance, cloud computing has transformed the way we store, access, and share data, but it has also introduced new vulnerabilities to widespread disruptions if we do not protect our cloud environments adequately.

b. Additionally, as our supply chains grow in complexity and scale, cyber threat actors can exploit such interdependencies to target organisations by exploiting weak links and trusted relationships in the supply chain.

6. Third, we have also observed that the techniques of malicious actors have grown in sophistication.

a. For example, ransomware groups are developing more sophisticated and effective methods to increase payouts, such as multilevel extortion techniques. Beyond the usual modus operandi of encrypting the targeted organisation's files and demanding payment in exchange for access restoration (the single

extortion technique), threat actors have started to integrate additional threats to the process to pressurise victims to make payment. This increases the severity of the threat of ransomware to all organisations.

7. Against such a backdrop, it is our duty as cybersecurity practitioners and leaders to stay ahead of these threats and safeguard our organisations and society as a whole. While the Government will do our part to support the efforts of organisations and individuals, all of us must do our parts.

8. On our part, we have developed several initiatives, at various levels, to support the security and resilience of our digital economy.

a. First, to improve cybersecurity and trust at the ecosystem-level, we have implemented the Cyber Trust and Essentials Marks and the CISOs-as-a-Service scheme.

b. Second, at the product-level, to support businesses in their efforts to develop and stand out with cyber secure and trusted products, we have introduced the Cybersecurity Labelling Scheme (CLS).

c. Third, at the individual-level, to nurture trusted cybersecurity professionals, we are exploring the feasibility of setting professional standards for our cybersecurity workforce.

d. Let me talk about these initiatives.

<u>Improving cybersecurity and trust at the ecosystem-level</u>

9. The Government has introduced several initiatives to improve our collective cybersecurity and trust at the ecosystem-level.

10. One, we are scaling up the Cyber Essentials and Trust Marks. These marks certify that organisations have invested in cybersecurity and are committed to protecting their own and their customers' systems and data. Since their launch in 2022, these Marks have seen encouraging adoption. More than 150 companies have been certified or are in the process of being certified.

11. We continue to work with our certification partners and other organisations to improve the adoption of these Marks. For instance, TUV SUD, one of our accredited certification bodies, and Lazada, a regional e-commerce platform, formed a strategic partnership last month, to advocate for the adoption of these Marks to Lazada's key partners, growing the cyber resilience of Lazada's partner ecosystem.

12. Two, at this year's Committee of Supply Debate, I announced the CISOs-as-a-Service scheme to help SMEs access cybersecurity consultancy services.

a. These CISO-as-a-Service providers will conduct a cyber health "checkup" of the companies and develop tailored Cybersecurity Health Plans to close cyber hygiene gaps, improve the companies' cybersecurity posture and work towards obtaining the Cyber Essential or Trust Marks.

b. Eligible SMEs will receive up to 70% funding support from the government.

c. Applications for the scheme is now open, and SMEs can easily apply through IMDA's CTO-as-a-Service platform as a single shopfront.

13. This is important. SMEs do face challenges in being more cyber secured. And oftentimes, they don't even know where to start. CISO as a service scheme would thus present a great opportunity for SMEs to gain easy access to services, products, and even resources to help become more cyber secure. And the Government is prepared to fund up to 70% for them to embark on this journey.

14. I encourage all of you, as cybersecurity leaders, to work with us to improve the cybersecurity posture of your organisations and your partner and vendor ecosystems, and help us build trust at the ecosystem-level.

<u>Supporting businesses in their efforts to develop and stand out with cyber secure and trusted products</u>

15. At the product-level, given the wide variety of products in the market, we have also observed that it is difficult for consumers to make informed decisions and choose products that are cyber secure. That is why we introduced the Cybersecurity Labelling Scheme, or CLS. This scheme bridges the information asymmetry gap and allows manufacturers of products with good cybersecurity provisions to stand out from their competitors, by enabling consumers to easily identify these products and make informed decisions.

a. First introduced in 2020, we have since expanded the scheme to include all categories of consumer Internet-of-Things devices, such as IP cameras, smart door locks and smart lights.

b. Today, there are more than 280 product manufacturers onboard this scheme.

c. There is mutual recognition of the CLS with other cybersecurity labelling schemes, in Germany and in Finland, which further improves its value to manufacturers.

d. I also note that the US recently announced the launch of its voluntary cybersecurity labelling program for smart devices - the "US Cyber Trust Mark" - to be implemented in 2024. With the US signalling that it is open to mutual recognition with similar labelling schemes, we can explore mutual recognition of our schemes.

16. Coming on board the CLS service in Singapore opens opportunities for manufacturers to other mutual recognitions around the world. I encourage you to utilise the CLS to allow your cyber secure products to stand out from your competitors, both in Singapore and internationally.

Nurturing trusted cybersecurity professionals

17. At the individual level, the Government recognises that the cybersecurity domain offers good career pathways and meaningful jobs.

18. Our cybersecurity workforce has more than doubled from 4,000 in 2016 to over 11,000 in 2022. While we continue to train more cybersecurity professionals, it is not just about the quantity but also the quality. There is a certain degree of expectation on cybersecurity professionals in terms of their standards and standing. We need to ensure that they have the requisite ethics, knowledge and skills for their work.

19. CSA introduced a licensing framework for cybersecurity service providers providing penetration testing and managed security operations centre monitoring services last year. This aims to safeguard consumers' interests and reduce the safety and security risks that cybersecurity service providers can pose. We have licensed close to 600 operators to-date.

20. We aim to develop a high quality trusted cyber workforce, to support the drive towards better quality and delivery of cybersecurity services and products, enhancing Singapore's position as a trusted business hub.

21. Going forward, CSA intends to work with the industry and professional associations to explore ways to further raise the quality and standing of cybersecurity professionals. We will continue to strike a good balance between cybersecurity needs and industry development.

Conclusion

22. To close, I would like to emphasise that cybersecurity is a collective responsibility. No one stakeholder, including the Government, can do it alone.

a. As cybersecurity leaders, each one of you plays a crucial role in protecting our digital ecosystem, and creating trust in the digital economy.

b. Let us collaborate, share knowledge, and work together, to address evolving cyber threats, create a safe cyberspace, and build a secure and vibrant digital future for all.

23. I wish everyone a fruitful time at the event. Thank you.

+++