

**VIRTUAL KEYNOTE ADDRESS BY SENIOR MINISTER OF STATE,
COMMUNICATIONS & INFORMATION DR JANIL PUTHUCHEARY
AT LAW SOCIETY'S CYBERSECURITY AND DATA PROTECTION
CONFERENCE 2022 AT 9.40AM**

"Building a safer Smart Nation": where we are and how we can work together

President of the Law Society of Singapore, Mr. Adrian Tan

Distinguished guests

Law Society members, speakers and panelists

Ladies and gentlemen

1. Good morning. Thank you to the Law Society for inviting me to this year's Cybersecurity and Data Protection Conference. I am delighted to be able to join all of you today for this important topic.

Building a safer Smart Nation

2. In our aspirations to become a Smart Nation, we want to better harness technology for growth, prosperity and human flourishing.

3. However, greater digitalisation also comes with greater risks. Two recent incidents underscore how events in the cyberspace can potentially have drastic impact on our daily lives.

- a. Between 2019 and late 2020, hackers exploited a vulnerability in a widely used network management software called SolarWinds. This allowed them to implant a backdoor and gain access to sensitive information and systems of about 18,000 organisations. The breach was significant not only in terms of

its scale, but also its ability to evade detection by directly targeting cybersecurity software.

- b. Last year, the IT systems of one US's most vital oil pipeline – Colonial Pipeline – were infected with ransomware. This led to the shutting down of pipelines all along the US East Coast, affecting access to petrol, jet fuel and home heating for thousands of airlines and consumers.

4. When the digital world promises so much, it is easy to think of cybersecurity and data protection as obstacles or barriers that stand in tension to the benefits of digitalisation, or a cost to innovation and economic interests from a business perspective. But the truth is, none of benefits of digitalisation can be harnessed if we are the victims of debilitating cyber-attacks that disrupt our essential services, or if our companies are regularly held at ransom by malicious actors. All of these incidents erode the trust that is essential for the realisation of the benefits of our digitalisation. **We must therefore think of cybersecurity and data protection as enablers – things that we must do so that good things, like economic growth and human flourishing can continue to take place in the digital space.**

5. In today's keynote, I want to share what we are doing today to address cybersecurity risks to Singapore, and how we can work together.

Three key approaches to address cybersecurity risks in Singapore

6. **The first area that we are actively looking at is to ensure that our laws can keep up with evolving technologies and cybersecurity threats.** The Cybersecurity Act currently provides us with a legal framework to secure and protect our Critical Information Infrastructure, which are key to delivering essential services such as water and power. This is currently being reviewed and we are planning to expand the Act's mandate to cover foundational digital infrastructure and key digital services. These are important enablers for our digital future, as more transactions and communication will take place online.

7. But given the global and cross-border transnational nature of cyber threats, we need to look beyond our borders and shape rules, norms and standards at the international level. A rules-based multilateral order in cyberspace is vital to foster trust and confidence between States and ensure that we have an open, stable, secure and interoperable ICT environment. This ensures that the cyberspace will not be a domain where might makes right.

- a. We have been actively participating in cyber discussions at the United Nations through the inaugural UN Open-Ended Working Group (OEWG) and the sixth UN Group of Governmental Experts (GGE). We are part of the process to negotiate and seek adoption of the consensus reports and re-affirm the UN Member States' commitment to the cyber stability framework.
- b. Since last year, Singapore's Permanent Representative to the UN in New York Ambassador Burhan Gafoor has also been the Chair of the OEWG on Security of and in the use of ICTs.

Our chairmanship will allow us to contribute constructively and make further progress in the next tranche of UN cyber discussions.

8. Laws and regulations are one approach in our toolkit. We also need and want to empower all enterprises and individuals to take greater ownership over their digital safety and security. All of us have a stake in making the online community safe for all Singaporeans.

9. As part of the broader Safer Cyberspace Masterplan, we have launched the SG Cyber Safe programme last year to help enterprises strengthen their cybersecurity awareness and adopt appropriate cybersecurity measures.

- a. It can be confusing for enterprises to navigate through the various cybersecurity measures and solutions, especially for those that are just starting out on this journey. For this reason, our initiatives such as the Cybersecurity Toolkits provide tailored guidance for different enterprise stakeholders.
- b. We also want to promote greater trust and transparency between enterprises and their vendors and suppliers, particularly since these third parties can be an additional source of cybersecurity risks. Our Cyber Essentials and Cyber Trust marks are good ways to provide assurance that their customers' data and IT systems are well protected.

10. Besides enterprises, all of us, as internet users and consumers, also play an important role in practising good cyber hygiene. Last year, we

embarked on our national awareness campaign called “Better Cyber Safe Than Sorry”. This campaign shares ways through which we can better protect our personal data and devices.

- a. We will be pushing out more campaign publicity on social media platforms and television channels later this year.

11. One common theme across all our initiatives is that the Government cannot do everything on our own. Cybersecurity is a team sport, and public-private partnerships are key to address emerging and evolving threats.

12. One group of partners that we have been working closely with are local hardware manufacturers. Together, we have developed the Cybersecurity Labelling Scheme (CLS) to help consumers make more informed decisions when purchasing computer products.

- a. Consumers and manufactures have shown support for CLS. There are now close to 150 products on the scheme, including smart home appliances and smart locks, and we expect many more coming onboard in the following months.

13. We see the legal fraternity as a key partner in cybersecurity as well.

- a. In our review of the Cybersecurity Act, we will consult with a wide range of stakeholders on the proposed amendments, given that the changes will have uneven impact across different industries. We will seek the legal industry’s views and my colleagues will share more details with you in due course.

- b. Many of you in the audience will also collect commercially sensitive information that need to be protected. As trustees and guardians of these data, we encourage firms in the legal fraternity to consider attaining the Cyber Essentials and Cyber Trust marks, which will provide added assurance for your clients. The certification will also be a good way to differentiate yourself from your competitors.

- c. We are glad that the Law Society has been supportive of our efforts to uplift cybersecurity for local enterprises and is on board the SG Cyber Safe Partnership programme to drive this collectively.

Conclusion

14. It is important for us to tap on each other's expertise in order to tackle more complex cybersecurity challenges. This is why I believe that conferences such as this are important, because it facilitates conversations across the various professions and allows for ideas to be exchanged freely.

15. All of you are attending today's conference because you have a professional or personal interest in cybersecurity or data protection. I will therefore encourage everyone in the audience – regardless of your seniority or role in your company – to be that driver of change and promote good cyber practices within your team or your organisation. I hope that you will find today's panel discussions meaningful and insightful.



Ministry of Communications
and Information

An Engaged and Connected Singapore

16. Thank you very much.