

## **SPEECH BY MOS TAN KIAT HOW AT THE LAUNCH OF SG CYBER SAFE PARTNERSHIP PROGRAMME ON 7 OCTOBER 2021, 1030AM**

### **“FOSTERING PUBLIC-PRIVATE COLLABORATIONS TO HELP BUSINESSES STAY CYBER-SECURE IN THE COVID ENDEMIC FUTURE”**

Industry partners  
Distinguished guests  
Ladies and gentlemen

#### **Introduction**

1. Good morning and welcome to the launch of the SG Cyber Safe Partnership Programme.

#### **Digitalisation presents business opportunities, but exposes enterprises to digital risks**

2. Digital technologies and platforms have proved indispensable for many businesses and their workers during this COVID-19 pandemic. In fact, the digitalisation trend has picked up pace with the onset of COVID-19. According to Enterprise Singapore (ESG), more than 3,500 Singapore businesses started digital transformation projects at the start of the pandemic in 2020, which is nearly 20% higher than the same period in the preceding year.

3. As more of our businesses seize the opportunities that come with digitalisation, they could have prioritised functionality and speed over security, which leaves them exposed to cyber threats. For example, the recent Singapore Cyber Landscape 2020 publication showed a 154% year-on-year increase in ransomware cases in 2020.

4. In recent months, we have seen reports of local enterprises hit by cyber-attacks. In June, a local consumer electronics retailer suffered a cyber-attack that led to a data breach of their customers' personal details, which was in turn used as blackmail. In a separate incident in August, a local eye clinic got hit by ransomware that compromised the personal data of more than 73,000 patients.

#### **The Government recognises the challenges faced by Small and Medium Enterprises when tackling cyber threats**

5. The increase in cyber-attacks underscores the importance of having adequate cybersecurity to safeguard businesses when they go online. However, we understand that it can be challenging for many Small and Medium Enterprises (SMEs).

6. We are also mindful that the pandemic has further created a challenging business environment where firms, especially SMEs, are resource stretched, having to manage a constantly evolving set of risk and uncertainties. Many are focused on keeping their operations going and delivering on their existing commitments.

7. We understand these constraints and have put in place measures to support our enterprises on their cybersecurity journey.

### **Raising cybersecurity awareness of enterprises**

8. First, the Government has developed a suite of toolkits to simplify cybersecurity for enterprises.

9. The toolkits are part of the *SG Cyber Safe Programme*, which was announced at my Ministry's Committee of Supply (COS) this year. The programme aims to raise enterprise cybersecurity awareness, and help them take action.

10. The toolkits are tailored for three important groups of users: (i) Enterprise leaders and SME owners, (ii) employees and (iii) IT teams in those businesses.

- a. The toolkit for enterprise leaders explains why upfront investment in cybersecurity makes good business sense as compared to taking remedial actions and/or making restitution when breaches occur. This toolkit is a starting point for the management team to develop the firm's cybersecurity strategy, work out its implementation approach and build a strong cybersecurity culture in the organisation.
- b. The toolkit for employees sets out how each person can exercise cyber safe behaviours in the work setting, such as setting strong passphrases to protect their digital assets and learning to be aware of common tactics used in phishing, so as not to fall prey to malicious cyber actors. Organisations can use the toolkit as a resource to conduct cyber awareness training for their employees. Many of these tips and good practices would also be useful for their employees in protecting themselves and their loved ones at home.
- c. The cybersecurity toolkit for IT and cybersecurity teams provides guidance on how they can find and prioritise resources to keep their enterprise IT systems safe. It will include technical tools that teams can adopt, such as simulating cybersecurity incidents to hone their responses during peacetime.

11. I am pleased to share that the toolkits for enterprise leaders and SME owners, as well as the toolkit for employees are now available for download on CSA's website from today<sup>1</sup>. The toolkit for IT teams will be progressively rolled out from next year. I encourage all enterprises, especially our SMEs, to make full use of these resources.

12. Another issue that many businesses are concerned with is data protection, which is closely linked to cybersecurity. To help enterprises better protect their data, the Personal Data Protection Commission (PDPC) recently launched a Guide that includes lessons learnt from past data breaches, and recommends a set of best practices that organisations can incorporate into their IT policies, systems and

---

<sup>1</sup> <https://www.csa.gov.sg/Programmes/sgcybersafe/toolkits>

processes. Enterprises can use this Guide together with the Cybersecurity toolkits that we are launching today.

### **Alleviating costs of adopting cybersecurity**

13. Having made a decision to raise its cybersecurity posture and developed a strategy to do so, many SMEs are often faced with the next set of difficult decisions around where to start and which solution to adopt. IMDA, with the support of CSA, has tried to make it easier for SMEs through the SMEs Go Digital programme.

14. Under this programme, SMEs can tap on cybersecurity solutions pre-approved by IMDA and CSA. Since the programme was launched in 2017, more than 5,000 SMEs have benefitted from these cybersecurity solutions. Examples include solutions that help enterprises to protect their end point devices, such as their desktops and laptops.

15. There are also more advanced solutions, such as unified threat management, for SMEs that may be more matured or have unique needs. The solutions are assessed to be market-proven, cost-effective and supported by reliable vendors. SMEs interested in adopting these solutions can apply for the Productivity Solutions Grant (PSG), which can help to offset up to 80% of the costs of adopting these solutions.

16. CSA is continually improving the range of cybersecurity products offered under the SMEs Go Digital Programme. For instance, CSA is collaborating with local cybersecurity industry partners to architect an integrated and automated Security-as-a-Service solution that can help protect enterprise users from malicious cyber activities. The implementation of this solution, when ready, will simplify cybersecurity for the users, raise their cybersecurity posture, and better protect users from the myriad of evolving cyber threats.

### **Public-private collaboration is key in reaching out to enterprises**

17. Recognising the importance of cybersecurity to our economy and society, the Government is putting in place measures to support our firms, as I have outlined earlier. However, our effort is necessary but insufficient. We need the wider ecosystem of firms to come together, including technology vendors, service providers and trade associations.

18. That is why CSA is launching the *SG Cyber Safe Partnership Programme* today. The programme aims to nurture this ecosystem of partners, starting with the 19 partners that have agreed to come onboard.

- a. CSA will work with technology vendors to align their products and/or solutions with our national cybersecurity effort. V-Key, for example, has plans to extend their identity solution as a multi-factor authentication solution for small enterprises. This helps to add an additional layer of protection to important accounts, such as administrator access to key systems in the enterprise.



- b. CSA will also partner service providers to protect their clients. One such example is Mastercard which has created the Mastercard Trust Centre, which incorporates cybersecurity advice for SMEs.
- c. CSA is also partnering trade associations such as the Singapore Business Federation to reach out to their members through events, webinars and information sharing.

19. The SG Cyber Safe Partnership Programme allows CSA to expand its reach to engage many more business, especially SMEs across various industry sectors. Our partners will benefit from this programme. They will be better plugged into the latest developments in the cybersecurity domain and get informed of latest advisories and guidelines from CSA. Through these engagements, our partners can also better add value to their clients and users.

20. On this note, I would like to thank our 19 early partners, who are here with us today. Thank you for your support and joining cause with the Government on protecting businesses and users online. I look forward to many more partners joining this programme. Interested organisations may visit CSA's website for more details.

## **Conclusion**

21. As Singapore transitions to living with endemic COVID-19, we must also be prepared for an increasingly digital way of life. We can do our part to stay cyber safe as we go digital. Enterprises should include cybersecurity into their overall business risk management and operations. Individuals, be it as employees, or in your own personal lives, need to stay vigilant about cybersecurity threats.

22. At the same time, we are as strong as our weakest link, particularly in an interconnected digital space. That is why we need to also work together – government and the private sector to secure our cyber space.

23. I welcome many more industry partners to join us in this important effort. Thank you very much.

--- END ---