Ministry of Communications and Information
An Engaged and Connected Singapore

Speech by MOS(CI) Tan Kiat How at the launch of CSA's Cyber Essentials and Cyber Trust marks on 29 March 2022 at 2.35pm

Industry partners
Distinguished guests
Ladies and gentlemen

Introduction

1. Good afternoon. I am happy to be here today to officially launch CSA's cybersecurity certification scheme – the Cyber Essentials and Cyber Trust marks.

Digitalisation presents tremendous opportunities for businesses, but also increases cyber risks

2. Digitalisation presents tremendous opportunities, but it also significantly increases our cybersecurity risks.

   a. For example, in June last year, hackers posted the data of some 700 million LinkedIn users on the dark web for sale[1].
   b. That is more than 9 in 10 of all LinkedIn members.
   c. The data leaked include the information of HR, finance and IT personnel who are often targets for phishing attacks.

3. Cyber-attacks are also becoming increasingly common in Singapore.

   a. In August last year, an insurance company here suffered a ransomware attack[2].
   b. In October, a healthcare platform's third-party vendor suffered a security breach, and it was discovered that patients' personal data including bank account information was compromised[3].
   c. And in January this year, a departmental store in Singapore also saw its customers' personal data leaked[4].

4. According to a CISCO survey of Asia Pacific businesses that was released last year, two in five SMEs in Singapore suffered a cyber incident over a period of 12 months from September 2020 to 2021[5].

5. The impact of a cyber-attack can be significant.

   a. It can be personal, in the case of data breaches;
   b. It can damage a company's reputation and business; and
   c. It can even bring down a country's critical infrastructure.

[1] Fortune article, "Massive data leak exposes 700 million LinkedIn users' information", June 30, 2021
[2] The Business Times, "Tokio Marine's Singapore unit hit by ransomware", 20 August 2021
[3] ZDNet.com, "Third-party data breach in Singapore hits healthcare provider", 26 October 2021
[4] The Straits Times, "Personal details of OG department store customers leaked in data breach", 7 January 2022
[5] Cybersecurity for SMBs: Asia Pacific Businesses Prepare for Digital Defense report by Cisco, September 2021

6. The average cost of a cyber-attack for companies in Singapore is approximately SGD1.7 million per breach[6], which could include the cost of revenue loss from disruptions to business operations and legal penalties when there is a data breach involving personal data.

   a. For some of our SMEs, this may be too high a cost to bear.
   b. That is why, it is critical for companies to be aware of cyber threats and implement the appropriate measures to counter them, even as they pursue digitalisation.

7. However, many SMEs have shared with us that they don't know where to start.

8. That is why CSA has developed a set of resources to help companies.

Three-pronged approach for companies to beef up their cybersecurity posture

9. Firstly, companies need to be aware that cybersecurity is not just a tech issue.

10. Cybersecurity awareness is essential at all levels within the company.

   a. Business leaders need to be aware of cyber risks and allocate sufficient resources for the IT teams to address them.
   b. In turn, IT teams need to put in place appropriate cybersecurity measures to protect the company.
   c. All employees need to be mindful of good cyber hygiene practices as they are the company's first line of defence.

11. CSA has developed a series of cybersecurity toolkits to help enterprise leaders, SME owners and employees learn about their specific roles in keeping their companies safe from cyber threats.

12. We launched these toolkits six months ago at the Singapore International Cyber Week. I am heartened to know that the toolkits have been downloaded over 3,200 times.

13. We have also added a toolkit for IT teams. It is now available on CSA's website.

14. I encourage all of you to make full use of these resources.

Recognising companies that put in place good cybersecurity measures

15. Secondly, customers want to be able to easily tell which companies have put in place good cybersecurity measures given the impact on them arising from personal data breaches and service disruptions.

16. They want to know whether firms have taken steps to prevent cyber-attacks, such as testing out various scenarios and preparing their business continuity plan.

17. In this regard, I'm happy to launch CSA's cybersecurity certification scheme for companies, comprising the **Cyber Essentials** and **Cyber Trust** marks.

18. The marks do not certify the cybersecurity of specific products or services. Rather, they certify the cybersecurity measures adopted at the organisation level.

[6] ChannelAsia's article "Security attacks cost Singaporean businesses $1.7M per breach", 21 January 2020

19. In developing the scheme, CSA referred to established international standards such as the ISO 27001, Service Organisation Control 2 and the US National Institute of Standards and Technology.

20. CSA piloted the certifications with companies from a wide range of sectors including Andersen's of Denmark Ice Cream, Kestrel Aero and Lazada Singapore who provided valuable feedback.

21. The pilot users found the certification useful in helping them identify their cybersecurity gaps. Importantly, they found the guidelines and process easy to follow and implement.

22. Companies should consider their risk profile when deciding which certification to go for. The Cyber Essentials mark may be more suitable for companies that have just embarked on their cybersecurity or digitalisation journey. It simplifies the approach by prioritising five cyber hygiene areas for companies to focus on.

23. However, if most of your business processes are digitalised, you probably have a higher cybersecurity risk profile as digital transactions form the core of your business. For such companies, the Cyber Trust mark may be more suitable.

24. The Cyber Trust mark takes on a tiered approach. There are five different cybersecurity preparedness tiers which address a broad spectrum of companies with different business operating models, such as the nature of your products or services, the industry you operate in, or the customers you supply to.

25. The Cyber Trust mark serves as a mark of distinction to prove that your company has put in place good cybersecurity practices and measures that are commensurate with your cybersecurity risk profile.

26. Companies that attain the Cyber Essentials or Cyber Trust mark can give their stakeholders and customers greater assurance and gain a competitive advantage in the market.

27. For instance, more multinational corporations are taking steps to protect against supply chain attacks. They may require their suppliers and vendors to demonstrate that they have implemented good cybersecurity practices. Our firms which are certified will have an advantage.

Supporting companies in their cybersecurity journey to attain the marks

28. Thirdly, firms, especially SMEs without dedicated IT or cybersecurity teams, have shared with us that it is challenging for them to navigate the many cybersecurity products and solutions out there.

29. To support our firms in their cybersecurity journey, CSA has brought together an ecosystem of partners that provide a suite of useful cybersecurity products and solutions.

30. These products and solutions include those that address the measures needed under the Trust marks. Others, like the cybersecurity-as-a-service providers, can help companies review their existing implementation and better prepare for their certification.

31. For companies that need help with data protection, some of these cybersecurity-as-a-service providers are also on IMDA’s Data Protection Essentials or DP Essentials programme that will be available from 1 April this year. This will ensure a more seamless experience for companies looking to address both cybersecurity and data protection needs.

32. Additionally, SMEs can make use of the Productivity Solutions Grant for selected cybersecurity products or solutions. Under the Grant, SMEs can get up to 70% support for qualifying cost.

Conclusion

33. In summary, CSA has worked closely with the cybersecurity industry to put in place a set of comprehensive measures to help our firms in strengthening their cybersecurity posture

a. First, developing a set of useful toolkits to guide our firms in starting or progressing in their cybersecurity journey.
b. Second, introducing the Cyber Essentials and Cyber Trust marks to help consumers identify firms that have put in place the necessary cybersecurity practices and measures.
c. Third, curating an ecosystem of partners that provide a suite of cybersecurity products and services that may be useful for our firms.

34. All firms, large and small, face the threat of cyber-attacks. I encourage all firms to take these risks seriously and make full use of the resources.

35. Let us work together to create a safe cyberspace and a vibrant and secure digital future for all. Thank you.