Ministry of Communications and Information
An Engaged and Connected Singapore

KEYNOTE ADDRESS BY MR TAN KIAT HOW, SENIOR MINISTER OF STATE FOR COMMUNICATIONS AND INFORMATION, AT SINGAPORE INTERNATIONAL CYBER WEEK (SICW)'S SG CYBER SAFE FOR ENTERPRISES EVENT ON 17 OCTOBER 2023, 2.00PM

Distinguished Guests

Ladies and Gentlemen

A very good afternoon

Introduction

1. Small to Medium Enterprises (SMEs) are important to our economy. 99% of enterprises in Singapore are SMEs, and they account for 71% of total employment.[1] The Government has been supporting SMEs in their digitalisation journey through the SMEs Go Digital programme so that they remain competitive and continue to provide good jobs for Singaporeans.

2. While digitalisation can unlock new opportunities for businesses, it also exposes them to new risks such as cyberattacks and cybercrimes. Therefore, as part of the Safer Cyberspace Masterplan, CSA has been supporting firms to enhance their cybersecurity by providing resources such as toolkits and establishing standards such as Cyber Essentials and Cyber Trust.

The Government is empowering enterprises to better manage their cyber risks

3. At the same time, we recognise that the digital space is evolving rapidly. We need to continually upgrade and update our playbook to keep up with technological developments like cloud services and generative AI, and the new set of cyberthreats that they bring about.

4. Working with like-minded ecosystem partners, CSA will do more to help enterprises better manage their cyber risks in three areas:

   a. First, by ensuring cybersecurity is considered when firms adopt emerging technologies like cloud services.

   b. Second, in protecting our firms from common cyberthreats like ransomware.

   c. Third, in empowering firms to take steps to assess and improve the cybersecurity of their online presence.

5. Let me touch on these three areas in turn. First, to empower enterprises to secure their use of emerging technologies, we are starting with cloud services.

6. Cloud services offer businesses many benefits. They can subscribe to more computing power or storage when needed, and cloud service providers typically offer a range of flexible options for add-on services to suit different needs. IMDA's Annual

[1] SingStat Enterprise Landscape by SMEs and Non-SMEs.

Survey on Infocomm Usage by Enterprises found that in 2022, nearly a third of Singapore's businesses were using cloud computing services[2].

7. While cloud solutions outsource the hosting of the environment, this does not mean that their security is guaranteed. Cybersecurity firm CrowdStrike reported that between 2021 and 2022, there has been 95% increase in cloud exploitation, and threat actors targeting cloud environments have nearly tripled.

8. Although cloud service providers are responsible for the security of the cloud, enterprises need to ensure their own security *within* the cloud. This means that enterprises still need to implement the necessary security controls and configurations to protect their digital assets on the cloud.

9. However, moving a company's digital infrastructure and services to the cloud entails significant adjustments to the company's security processes. Many companies do not have the know-how to shift to the cloud safely and securely. To support such companies, CSA will be releasing the Cloud Security Companion Guides to complement our suite of Cyber Essentials and Cyber Trust standards.

10. If you are a smaller enterprise, the Companion Guide for Cyber Essentials is designed for your needs. When subscribing to cloud services, you may refer to the Guide as you configure your cloud-based Software-as-a-Service solutions. Larger organisations that are shifting to the cloud can refer their IT teams to the Companion Guide for Cyber Trust. The Guides have been prepared in partnership with the Cloud Security Alliance and include platform specific guides for major cloud service providers like Amazon Web Services, Google Cloud, and Microsoft Azure. CSA is working with other providers, such as Huawei, to develop more platform specific guides.

11. Second, CSA will empower enterprises, especially SMEs, to better protect themselves against ransomware. In 2022, 132 ransomware cases were reported to SingCERT. Of this figure, more than 100 were reports made by SMEs, specifically in the manufacturing and retail sectors.[3] Ransomware is a huge threat that enterprises face, especially smaller firms.

12. In the Singapore Interagency Counter Ransomware Task Force report released last year, the task force recognised that it can be difficult to find useful information on ransomware prevention and response given the pace at which the ransomware threat evolves. This knowledge gap could be one reason why our enterprises are falling victim to ransomware.

13. I am therefore pleased to announce the launch of Singapore's Ransomware Portal by the Singapore Police Force (SPF), in collaboration with CSA. The Portal is a one-stop platform for organisations to access ransomware-related resources.

14. It provides victims of ransomware attacks with recovery support such as known decryption keys and incident response checklists. The website also publishes alerts and advisories on preventive measures, and information on global trends and emerging ransomware variants.

[2] 27% of respondents, IMDA Annual Survey on Infocomm Usage by Enterprises 2022.

[3] CSA's Singapore Cybersecurity Landscape 2022

15. For an organisation that falls victim to a ransomware attack, it can use this portal to report incident to the authorities, find information on how it should respond, and learn more about preventing such attacks in future. This one-stop portal will make all ransomware-related information convenient for all to access, so that enterprises can be better supported to defend against such attacks.

16. Third, CSA will empower enterprises to evaluate and benchmark their own internet hygiene. The internet hygiene, in other words website and email domain security, can affect a business' reputation. Compromise of webpages could cause reputational damage and erode the trust of customers, partners, and shareholders.

17. According to CSA's Singapore Cyber Landscape 2022, the majority of website defacement incident victims reported to SingCERT were SMEs[4]. Many SMEs find it challenging to evaluate and fix the security of their website and email domains as it requires some technical knowledge and resources.

18. CSA offers the Internet Hygiene Portal for organisations to evaluate their website and email domain security. Users on the portal can provide the domain name of a website or email address and get immediate feedback on its internet hygiene status, along with suggestions on areas for improvement.

19. To recognise enterprises with good internet hygiene, CSA has also launched Internet Hygiene Rating (IHR), tables which cover platforms used in sectors like Ecommerce and Healthcare so that they can better benchmark themselves against their peers.

20. I am pleased to announce that we are publishing a new IHR table for Infocomm Technology providers that specialise in website and email management.

21. This table recognises strong website and email hygiene for local vendors which manage, configure, and remediate their clients' digital services. Enterprise clients can also refer to the information in this table when selecting their Infocomm Technology providers.

The Government is also working with industry partners to promote good cybersecurity in key sectors

22. CSA will be shifting its emphasis in the next phase of the SG Cyber Safe Programme for enterprises. Beyond broad-based initiatives to raise cybersecurity amongst firms, moving forward, CSA intends to work closely with key sectors to improve their cybersecurity posture. And we are starting with healthcare and manufacturing as the first two key sectors. Let me just briefly mention them in turn.

23. Healthcare is an essential service, and digitalising the provision of healthcare services offers new opportunities in patient management, including better user experience for patients. However, healthcare data is highly sensitive and confidential, and is a prime target of cyber criminals.

24. This is why the Cyber Essentials standard, which is broad-based, has been adapted for Clinic Management System (CMS) vendors. Patients will have greater assurance that certified vendors of the CMC have taken steps to secure their data. That is one

[4] CSA's Singapore Cybersecurity Landscape 2022

example of how CSA is working with our healthcare partners to improve the cybersecurity standards.

25. Next, manufacturing is the largest contributing sector to Singapore's economy, accounting for more than 20% of our GDP in 2022.[5] As more businesses in this sector seek to upgrade or automate traditional manufacturing practices using digital technologies, we want to ensure that the sector is equipped to manage cyber risks. This is especially when many of the equipment and systems are not purely digital systems, but are what we call Operation Technology (OT) systems.

26. CSA will be partnering with the Singapore Manufacturing Federation (SMF) to improve cybersecurity in this sector. As a start, SMF will work with CSA to raise awareness on cybersecurity amongst its members.

27. I am glad to know that CSA's partners in the healthcare and manufacturing sectors welcome this sector-specific support. There is a strong demand for sector-specific cybersecurity initiatives to account for their different operating contexts. CSA will explore extending such sector-specific support to other key sectors.

Conclusion

28. I will conclude my remarks by recognising the important role that all employees play in defending their companies from cyber threats. Verizon's 2023 Data Breach Investigations Report described 74% of breaches as involving the human element, which includes social engineering attacks, errors, or misuse.

29. It is crucial that organisations drive awareness on cybersecurity throughout their ranks, as this can make a meaningful difference in detecting and preventing cyberattacks. This is why CSA will be signing a partnership agreement with NTUC Learning-Hub, to deliver cybersecurity awareness courses for the employees of organisations of all sizes. By empowering enterprises and their employees, our cyberspace will be safer and more secure. Sector-specific initiatives complement these efforts.

30. I thank all of you again for being part of this journey to secure our cyberspace, by working together and taking a whole-of-society, whole-of-nation approach to ensure that our cyberspace remain secure and safe, and to build trust in a digital economy. We look forward to continuing to work alongside the industry to maintain Singapore's cybersecurity posture. Thank you.

+++

[5] 21.6%, SingStat