MEDIA FACTSHEET

KEEPING OUR DIGITAL SPACES SAFE

1. As Singapore continues to move towards being a Smart Nation and a Digital Economy, there is an even greater need for us to strengthen our cyber defences and to safeguard ourselves against an evolving threat landscape. Keeping our digital spaces safe will continue to be a priority for the Ministry of Communications and Information (MCI) in 2021.

SG Cyber Safe Programme

2. The Cyber Security Agency of Singapore (CSA) will launch the SG Cyber Safe Programme to help Singapore enterprises to raise their cybersecurity posture. The programme is part of the Safer Cyberspace Masterplan launched in October 2020, which aims to raise Singapore's general level of cybersecurity.

3. The SG Cyber Safe Programme is a concerted effort by the Government to help enterprises better protect themselves in the digital domain. Under this programme, a slate of initiatives will be introduced. These include:

a. Cybersecurity toolkits. The toolkits, targeted at key enterprise stakeholders such as enterprise leaders, technical teams and employees, will provide leaders with a deeper understanding of cybersecurity issues and threats. It will also enable them to implement cybersecurity measures, including employee training, within the organisation.

   CSA will be rolling out the employee cybersecurity toolkit by the end of 2021. For a start, CSA has worked with Smart Nation and Digital Government Group (SNDGG) and Civil Service College (CSC) to adapt existing cybersecurity modules - originally developed for public officers - for employees in the private sector.

b. Tools for enterprises to self-assess their cybersecurity posture. This includes the Exercise-in-a-Box Singapore incident response simulation tool, which will be launched in partnership with the United Kingdom's National Cyber Security Centre in the later half of 2021. CSA will also develop assessment tools on enterprises' Internet domain, connectivity and email health.

c. SG Cyber Safe Trustmark. The Trustmark will serve as a mark of distinction for enterprises that have put in place good cybersecurity measures that correspond to their risk profiles.

   CSA will start industry consultations on the SG Cyber Safe Trustmark from April 2021 to seek views on the concept and implementation. CSA intends to introduce the trustmark by early-2022. As the trustmark is intended for companies and/or projects with higher cyber risk, a separate cyber hygiene mark will also be developed to complement the SG Cyber Safe trustmark. More details on the trustmark and cyber hygiene mark will be announced in due course.

Critical Information Infrastructure (CII) Supply Chain Programme

4. CSA will also launch the Critical Information Infrastructure (CII) Supply Chain Programme to enhance the security and resilience of Singapore's CII sectors[1]. Led by CSA, the programme is a national effort to establish processes and best practices to help CSA, CII owners (CIIOs) and their vendors manage supply chain risks holistically, and strengthen their overall supply chain cybersecurity posture.

5. Most organisations engage vendors to supply and deliver their products and services. Malicious actors may exploit the supply chain ecosystem to infiltrate an organisation in order to steal data or cause service disruptions. Securing the supply chain can be a challenging task as vulnerabilities could be introduced at any point in the supply chain and these vulnerabilities may be hard to detect.

6. Managing supply chain cybersecurity risks is a collective responsibility of all stakeholders. For CIIOs, the CII Supply Chain Programme will develop guidelines to enable them to better understand and manage their vendors. This includes mapping their vendors based on the services provided and ranking them by their cybersecurity posture. For vendors, it will also enable them to maintain an adequate level of cybersecurity. This will be done through implementing measures proposed by the CIIOs and timely reporting of progress.

7. The CII Supply Chain Programme will be guided by three key principles to manage supply chain cybersecurity risks, namely:

a. Assurance. This includes policies and processes to be implemented by CIIOs and their vendors to provide adequate levels for cybersecurity. For instance, CIIOs and vendors would be required to conform to security requirements in accordance to best practices and international standards.

b. Transparency. This includes the introduction of reporting mechanisms that reveal the extent to which vendors meet their assurance commitments and contractual obligations. Should a vendor be unable to fulfil the requirements at any point in time, they would be required to formulate mitigating measures to address the gaps.

c. Accountability. This could involve invoking consequences, such as payment for damages or termination of contracts, for failure to meet assurance or transparency requirements.

8. More details on the CII Supply Chain Programme will be announced in the third quarter of 2021.

[1] The 11 sectors are Government, Security & Emergency, Healthcare, Media, Banking & Finance, Energy, Water, Infocomm, Maritime, Aviation and Land Transport