Technology, Media & Telecommunications

Singapore's Cybersecurity Regime Set to Undergo Update – Cybersecurity (Amendment) Act Introduced in Parliament

Introduction

The Cybersecurity Act was enacted in 2018 to regulate cybersecurity threats and incidents, critical information infrastructure ("**CII**"), and cybersecurity service providers. Since then, there have been significant changes in the cyber threat landscape, as well as in the technological operating context. To keep pace with these changes, the Cybersecurity Agency of Singapore ("**CSA**") has introduced the Cybersecurity (Amendment) Bill ("**Bill**"), which was introduced in Parliament for its first reading on 3 April 2024.

The Bill seeks to update the Cybersecurity Act to remain fit-for-purpose in light of emerging threat factors and operational practicalities. The main amendments in the Bill include the following:

- Updating existing provisions relating to the cybersecurity of CII;
- Expanding CSA's oversight to cover the cybersecurity of Systems of Temporary Cybersecurity Concern ("**STCC**"); and
- Creating two new classes of regulated entities – Entities of Special Cybersecurity Interest ("**ESCI**") and Foundational Digital Infrastructure ("**FDI**").

CSA had earlier conducted a public consultation on the draft Bill from 15 December 2023 to 15 January 2024. For more information on this, please see our earlier Legal Update on the public consultation here. CSA has now published a Closing Note to the Public Consultation on the Cybersecurity (Amendment) Bill ("**Closing Note**"), summarising the feedback received and CSA's response to the feedback.

This Update highlights some of the key features of the Bill and its proposed amendments, as well as CSA's insights on the operation of the Bill's provisions and its intentions for future engagement with stakeholders as set out in the Closing Note.

Critical Information Infrastructure

CII are computers or computer systems that are necessary for the continuous delivery of essential services, such as water, electricity, and banking services. Currently, the cybersecurity of CII is provided

for under Part 3 of the Cybersecurity Act, which sets out the obligations and responsibilities of owners of designated CII.

The amendments in the Bill recognise new technological and business models in the CII framework. For example, CII owners are utilising a wider and more sophisticated range of distributed system architecture (such as cloud computing); the Bill thus seeks to ensure CII owners remain responsible for the cybersecurity of their CII and have additional obligations to report cybersecurity incidents that happen in their supply chains. Further, with the advancement of virtual computing, essential service providers are increasingly relying on outsourced CII to deliver essential services, which means that the essential service provider may not be the owner of the CII; the Bill thus seeks to address the responsibilities of such essential service providers.

The Bill divides the CII cybersecurity framework into two categories:

- Provider-owned CII, where the essential service provider is the owner of the CII; and
- Providers of essential services ("**PES**") that depend on third-party-owned CII for the delivery of the essential services.

Provider-owned CII

Part 3 of the Cybersecurity Act will continue to govern provider-owned CII. However, the responsibilities of the owners of such CII will be enhanced.

For example, owners of provider-owned CII are currently required to report prescribed cybersecurity incidents to the Commissioner of Cybersecurity ("**Commissioner**"). The Bill will introduce new categories of cybersecurity incidents that must be reported to the Commissioner – in particular, incidents that occur in their supply chain. The new categories are:

- Prescribed cybersecurity incidents in respect of any computer under the control of the owner, where the computer is not interconnected with, and does not communicate with, the provider-owned CII; and
- Prescribed cybersecurity incidents in respect of any computer under the control of a supplier to the owner that is interconnected with, or that communicates with, the provider-owned CII.

CSA has stated in the Closing Note that, in order to help CII owners manage this compliance burden, it will work with CII owners to develop a pragmatic approach to the submission of incident reports before the requirements come into force.

Third-party-owned CII

The Bill will introduce a new Part 3A that allows the Commissioner to designate a PES as a designated provider responsible for the cybersecurity of third-party-owned CII.

The Commissioner may subject designated PES to duties relating to the cybersecurity of third-party-owned CII, including:

- Complying with relevant codes of practice, standards of performance or written directions;
- Notifying the Commissioner of prescribed cybersecurity incidents involving the third-party-owned CII; and
- Audits and risk assessments of the third-party-owned CII.

Under Part 3A, the designated PES will be required to obtain legally binding commitments from their computing vendor (the latter being the owner of the third-party-owned CII) to ensure that the PES is able to discharge its duties under the Cybersecurity Act, and that applicable cybersecurity standards will be maintained. If the PES does not obtain the required commitments, or the standards are not maintained, the Commissioner may order the PES to stop using the third-party-owned CII to deliver the essential services.

In the Closing Note, CSA clarified that the proposed amendments are not intended to regulate: (a) cloud service providers providing cloud solutions to support the CII; or (b) the computing vendors of a PES as CII owners. The statutory responsibilities imposed on a CII owner under Part 3, or a designated PES under Part 3A, cannot be passed on to the cloud service provider or the computing vendor.

As for the designation of a PES, CSA clarified in the Closing Note that designation will involve a considered process, which includes working closely with any parties that CSA identifies as a potential PES and the relevant sector regulator, before deciding if there is a basis to proceed with designation.

Systems of Temporary Cybersecurity Concern

In recognition of the fact that there may be times where certain systems are of higher risk due to temporary situations, the Bill will allow CSA to proactively secure STCCs, which are computers or computer systems (located wholly or partly in Singapore) where for a limited period the risk of a cyber-attack is high, and their loss or compromise would have a serious detrimental effect on the national security, defence, foreign relations, economy, public health, public safety or public order of Singapore.

An STCC may be designated as such for a period of no more than one year (although this may be extended). An example of an STCC would be the temporary systems used to support the distribution of critical vaccines during a pandemic.

Once designated, an STCC would be subject to several duties, including: (a) provision of cybersecurity-related information; (b) notification of prescribed cybersecurity events; and (c) compliance with codes of practice, standards of performance or written directions issued by the Commissioner.

Entities of Special Cybersecurity Interest and Foundational Digital Infrastructure

Apart from CII, CSA has recognised that there are other nationally-important computer systems and entities of special cybersecurity interest. The Bill thus introduces two new classes of regulated entities:

- **ESCIs** are entities that store sensitive information or use computers to perform a function which, if disrupted, is likely to have a significant detrimental effect on the defence, foreign relations, economy, public health, public safety or public order of Singapore. Examples of ESCIs could include autonomous universities.
- **FDIs** are services that promote the availability, latency, throughput or security of digital services. In particular, a major FDI provider is one that provides an FDI service to or from Singapore, where the impairment or loss of the FDI service could lead to disruption to a large number of businesses or organisations. This may include cloud service providers and data centres.

CSA has indicated that these new classes will be subject to a "light-touch" regulatory treatment, and that the obligations imposed will not be at the level of those imposed on CIIs.

Once designated as an ESCI or a major FDI service provider, the entity would be subject to several duties, including: (a) provision of cybersecurity-related information; (b) notification of prescribed cybersecurity events; and (c) compliance with codes of practice, standards of performance or written directions issued by the Commissioner.

CSA has communicated in the Closing Note that further industry consultations will be conducted on the development of the incident reporting parameters and applicable cybersecurity codes or standards for ESCIs / major FDI service providers. CSA will take reference from international best practices and work closely with sectoral regulators to harmonise any new sectoral regulations.

Concluding Words

The Bill sets out new and existing classes that will be subject to regulation under the Cybersecurity Act: (a) owners of provider-owned CII; (b) designated PES responsible for third-party-owned CII; (c) STCCs; (d) ESCIs; and (e) FDIs. The scope of the amendments demonstrates the speed at which the cybersecurity landscape is changing, and CSA's efforts at implementing comprehensive changes to the legislative framework in a prompt manner to remain up to date.

Technology, Media & Telecommunications

The CSA has said in its Closing Note that it remains committed to holding further industry consultations on the development of subsidiary technical and operational matters (such as the codes of practice and incident reporting parameters) and the operationalisation of the proposed amendments.

The proposed amendments in the Bill have far-reaching impact and operational implications, especially for organisations and businesses involved in the provision of essential services, their computing vendors, cloud service providers and data centre operators. It is therefore critical for potentially affected entities to carefully review the proposed amendments, and to proactively reach out to and engage the CSA on an urgent basis to shape the implementation of the proposed amendments. Entities should also start reviewing the steps that need to be taken to ensure compliance with the relevant duties and obligations, should the proposed amendments come to pass.

For more information, please feel free to contact our team below.

Contacts

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0751

rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0786

steve.tan@rajahtann.com

Benjamin Cheong
Deputy Head, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0738

benjamin.cheong@rajahtann.com

Tanya Tang
Partner (Chief Economic and Policy Advisor), Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

T +65 6232 0298

tanya.tang@rajahtann.com

Wong Onn Chee
Chief Executive Officer
Rajah & Tann Cybersecurity

T +65 6996 0404

onnchee@rtcyber.com

Click **here** for our Partners in Technology, Media and Telecommunications Practice.

Please feel free to also contact Knowledge Management at eOASIS@rajahtann.com

Our Regional Contacts

RAJAH & TANN SOK & HENG | *Cambodia*
Rajah & Tann Sok & Heng Law Office
T +855 23 963 112 / 113
F +855 23 963 116
kh.rajahtannasia.com

RAJAH & TANN 立杰上海
SHANGHAI REPRESENTATIVE OFFICE | *China*
Rajah & Tann Singapore LLP
Shanghai Representative Office
T +86 21 6120 8818
F +86 21 6120 8820
cn.rajahtannasia.com

ASSEGAF HAMZAH & PARTNERS | *Indonesia*
Assegaf Hamzah & Partners

Jakarta Office
T +62 21 2555 7800
F +62 21 2555 7899

Surabaya Office
T +62 31 5116 4550
F +62 31 5116 4560
www.ahp.co.id

RAJAH & TANN | *Lao PDR*
Rajah & Tann (Laos) Co., Ltd.
T +856 21 454 239
F +856 21 285 261
la.rajahtannasia.com

CHRISTOPHER & LEE ONG | *Malaysia*
Christopher & Lee Ong
T +60 3 2273 1919
F +60 3 2273 8310
www.christopherleeong.com

RAJAH & TANN | *Myanmar*
Rajah & Tann Myanmar Company Limited
T +95 1 9345 343 / +95 1 9345 346
F +95 1 9345 348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*
Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 8894 0377 to 79 / +632 8894 4931 to 32
F +632 8552 1977 to 78
www.cagatlaw.com

RAJAH & TANN | *Singapore*
Rajah & Tann Singapore LLP
T +65 6535 3600
sg.rajahtannasia.com

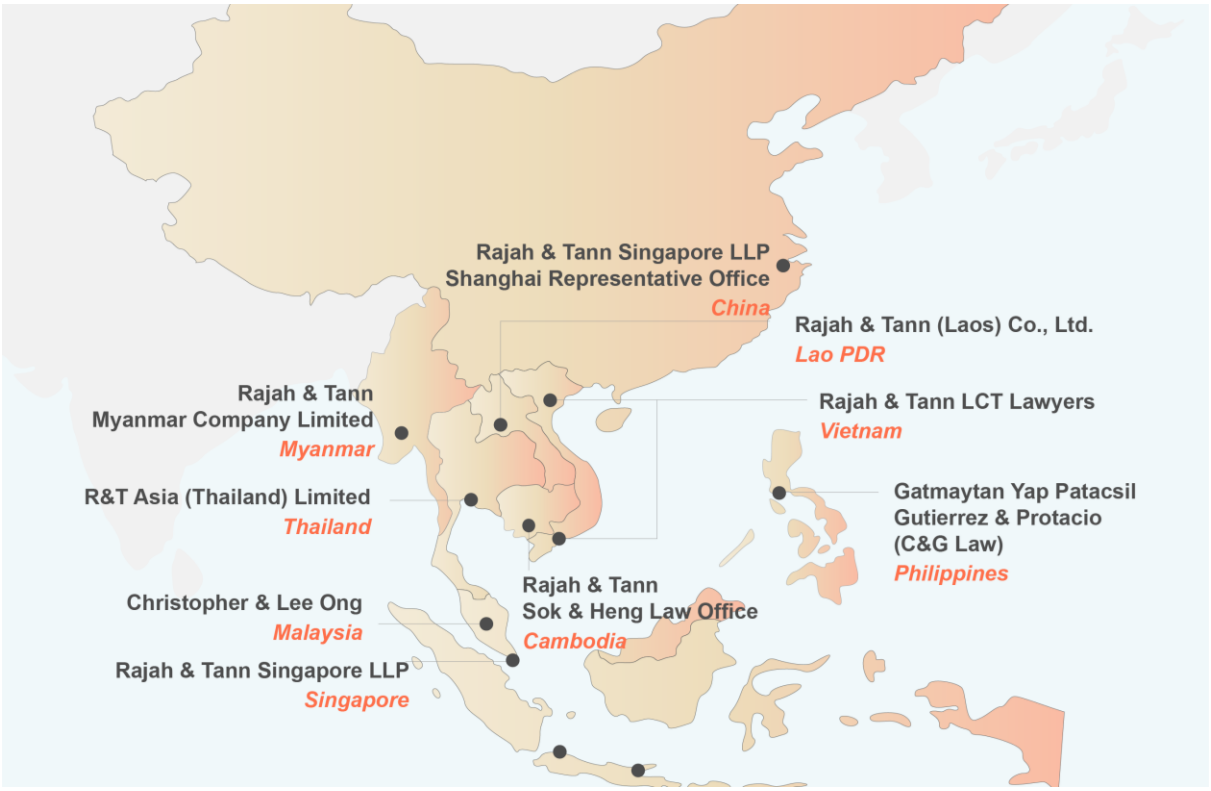
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

RAJAH & TANN LCT LAWYERS | *Vietnam*
Rajah & Tann LCT Lawyers

Ho Chi Minh City Office
T +84 28 3821 2382 / +84 28 3821 2673
F +84 28 3520 8206

Hanoi Office
T +84 24 3267 6127
F +84 24 3267 6128
www.rajahtannlct.com

Our Regional Presence



Rajah & Tann Singapore LLP is one of the largest full-service law firms in Singapore, providing high quality advice to an impressive list of clients. We place strong emphasis on promptness, accessibility and reliability in dealing with clients. At the same time, the firm strives towards a practical yet creative approach in dealing with business and commercial problems. As the Singapore member firm of the Lex Mundi Network, we are able to offer access to excellent legal expertise in more than 100 countries.

Rajah & Tann Singapore LLP is part of Rajah & Tann Asia, a network of local law firms in Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, the Philippines, Singapore, Thailand and Vietnam. Our Asian network also includes regional desks focused on Brunei, Japan and South Asia.