Technology, Media, And Telecommunications

Cybersecurity Bill Open for Public Consultation

Introduction

On 10 July 2017, the Ministry of Communications and Information ("**MCI**") and the Cyber Security Agency of Singapore ("**CSA**") jointly published the draft Cybersecurity Bill, and invited the public to provide feedback on the same by 3 August 2017.

The Cybersecurity Bill proposes to establish a framework for the protection and maintenance of national cybersecurity and critical information infrastructure ("**CII**") in Singapore, in line with the CSA's national mandate to prevent and respond to cybersecurity threats and incidents. There are four main objectives in introducing the Cybersecurity Bill:

(a) to impose and formalise the duties of CII owners in ensuring the cybersecurity of CII under their responsibility;

(b) to empower the CSA with the necessary powers to manage and respond to cybersecurity threats and incidents;

(c) to establish a framework for the sharing of cybersecurity information with the CSA; and

(d) to introduce a light-touch licensing framework for the regulation of certain cybersecurity service providers.

We elaborate on the measures introduced by the Cybersecurity Bill to meet these four objectives below.

Duties of CII Owners

Under the Cybersecurity Bill, CII is defined as a computer or computer system necessary for the continuous delivery of essential services which Singapore relies on. There are currently 11 critical sectors in which essential services have been identified: government; security and emergency; healthcare; telecommunications; banking and finance; energy; water; media; land transport; air transport; and maritime.

The CSA has the power to designate a computer or computer system as a CII, upon the provision of written notice to the CII owner. CII owners are then subject to various statutory duties, including a duty to provide information, a duty to report cybersecurity incidents and a duty to conduct regular audits of their CII, to ensure that they are responsible for the cybersecurity of the CII that they own.

It should also be noted that under the Cybersecurity Bill, CII owners will only be penalised for wilful failure to comply with their duties or the CSA's directions – they will not be directly penalised for cybersecurity breaches.

Powers of the CSA

The Cybersecurity Bill also proposes to empower the CSA with various powers, in order to allow it to effectively conduct cybersecurity investigations. The extent of the CSA's powers of investigation will depend on the severity of the situation:

(a) in relation to all cybersecurity threats and incidents, the CSA will have the power to examine anyone relevant to the investigation, and require the provision of relevant information;

(b) in relation to serious cybersecurity threats and incidents, the CSA will have the power to exercise more intrusive measures, such as powers to enter relevant premises and seize relevant computers or equipment; and

(c) in relation to emergency measures and requirements, the Minister can authorise any person or organisation to take any necessary measures to prevent, detect or counter a threat to a computer or computer service.

Cybersecurity Licensing Framework

In addition, in order to improve assurance on security and safety, raise quality and appreciation, and address information asymmetry, the Cybersecurity Bill purports to introduce a light-touch licensing framework for certain cybersecurity service providers.

Under the proposed licensing regime, two types of licences will be issued: (i) an Investigative Cybersecurity Service licence, for cybersecurity services which are investigative in nature; and (ii) a Non-Investigative Cybersecurity Service licence, for cybersecurity services which are not of an investigative nature.

The list of licensable cybersecurity service providers will be set out in a Schedule. At this stage, only penetration testing service providers and managed security operations centre service providers have been identified as being licensable. However, the licensing framework will not take immediate effect, and the CSA intends to have further consultation with the industry beforehand.

Our Comments

The Cybersecurity Bill represents a serious effort on the part of the Singapore government to deal with the rising spectre of cybersecurity threats and should be commended for its bold adoption of a whole of Singapore approach to the management of cybersecurity threats.

Specifically, some of the main key differences heralded by this approach that we observe are:

(a) the Cybersecurity Bill covers all types of data, and covers all types of information, as well as the computers and computer systems that store or process such information, unlike other legislation such as the Personal Data Protection Act ("**PDPA**") and Banking Act that impose information security requirements on a more selective basis;

(b) the Cybersecurity Bill will also apply to both public/governmental and private entities, unlike the PDPA;

(c) the Cybersecurity Bill appears to have a wider definition of "computer" as there are no expressly built in exceptions therein unlike the Computer Misuse and Cybersecurity Act ("**CMCSA**"). Further, "computer systems" under the Cybersecurity Bill also further expands the ambit of this legislation by including operational technology systems such as niche systems commonly found in public utilities; and

(d) the Cybersecurity Bill provides a new light touch licensing regime to ensure that the providers of cybersecurity services provide quality services.

Notwithstanding the laudable scope and intent of this bill, some uncertainties remain over the bill which will require clarification through this consultation process. Amongst these uncertainties are the following:

(a) whether the definition of "computers" includes mobile telecommunication devices such as mobile phones and tablets, which if so, will subject such devices to the investigative powers of the CSA during any cybersecurity incident;

(b) whether every CII will need to be designated by way of a written notice from the Commission before the obligations will apply to that CII (or whether it is for CII owners to self-assess whether their computer system etc. fulfils the criteria of critical information infrastructure and to take the initiative to approach the CSA for guidance where unclear). It may be the case that future subsidiary legislation will deal with this point;

(c) whether any commercially sensitive information disclosed to the CSA as part of the statutory obligations imposed by the Cybersecurity Bill will remain confidential;

(d) whether the licensing regime is intended to include vendors providing managed security services as a necessary ancillary service to their dedicated infrastructure and primary operations (eg. data centre operators);

(e) where a CII owner requires its upstream/downstream partners (e.g., the CII systems operator or cybersecurity service provider) to take certain action in order for the CII owner to comply with its obligations, whether the CII owner may disclose to third parties that its computer or computer system has been designated as a CII; and

(f) whether the 90-day timeframe to inform the CSA of any intended change in ownership of the CII under section 14 of the Cybersecurity Bill is consistent with other timeframes where other regulatory approval is required for changes in ownership.

Concluding Words

While the Cybersecurity Bill is expected to have the biggest impact on CII operators and providers of cybersecurity services, the imposition of the duties on CII operators are likely to trickle down to parties that make use of or interface with such CII as some of these duties may also be imposed on third parties. Hence, it may be possible that additional costs may be passed down to customers in terms of higher fees.

Nevertheless, the Cybersecurity Bill is timely as it seeks to deal with the realities of our present day interconnected world where data in computer systems are constantly at risk of attack or pilfering from cyber-criminals or other malcontents.

As we observed above, the Cybersecurity Bill is laudable for the holistic and comprehensive approach it adopts to tackling the issue of cybersecurity, but further clarifications in some areas are needed to address some latent uncertainties in the current draft.

Therefore, we strongly encourage all interested and potentially affected parties to carefully consider and respond to the proposals set out in the Cybersecurity Bill.

Please do not hesitate to contact us if you wish to discuss the issues raised herein or to respond to the public consultation.

Contacts

Rajesh Sreenivasan
Head, Technology, Media & Telecommunications

D (65) 6232 0751
F (65) 6428 2204
rajesh@rajahtann.com

Steve Tan
Deputy Head, Technology, Media & Telecommunications

D (65) 6232 0786
F (65) 6428 2216
steve.tan@rajahtann.com

Lionel Tan
Partner, Technology, Media & Telecommunications

D (65) 6232 0752
F (65) 6428 2119
lionel.tan@rajahtann.com

Benjamin Cheong
Partner, Technology, Media & Telecommunications

D (65) 6232 0738
F (65) 6428 2233
benjamin.cheong@rajahtann.com

Tanya Tang
Partner
(Chief Economic and Policy Advisor)
Competition & Antitrust and Trade

D (65) 6232 0298
F (65) 6225 0747
tanya.tang@rajahtann.com

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

Our Regional Contacts

RAJAH & TANN | *Singapore*

Rajah & Tann Singapore LLP
T +65 6535 3600
F +65 6225 9630
sg.rajahtannasia.com

R&T SOK & HENG | *Cambodia*

R&T 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) Sole 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 NK LEGAL | *Myanmar*

Rajah & Tann NK Legal Myanmar Company Limited
T +95 9 73040763 / +95 1 657902 / +95 1 657903
F +95 1 934 5348
mm.rajahtannasia.com

GATMAYTAN YAP PATACSIL
GUTIERREZ & PROTACIO (C&G LAW) | *Philippines*

Gatmaytan Yap Patacsil Gutierrez & Protacio (C&G Law)
T +632 894 0377 to 79 / +632 894 4931 to 32 / +632 552 1977
F +632 552 1978
www.cagatlaw.com

RAJAH & TANN | *Thailand*

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

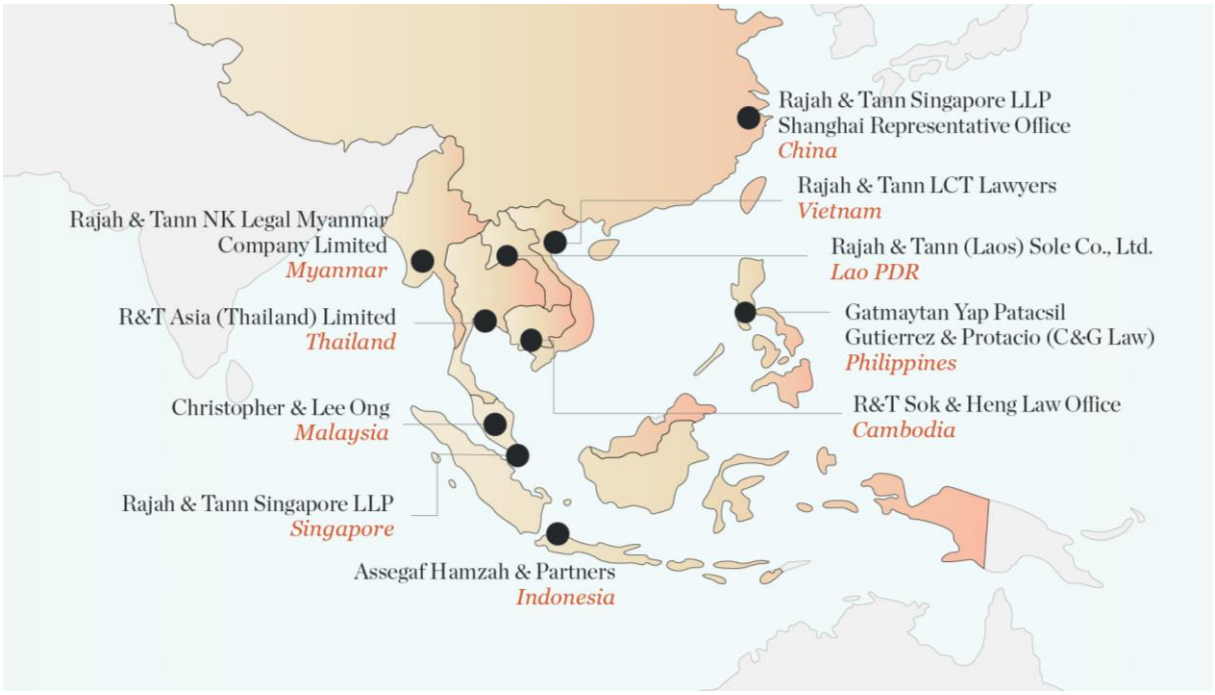
RAJAH & TANN LCT LAWYERS | *Vietnam*

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 Singapore, Cambodia, China, Indonesia, Lao PDR, Malaysia, Myanmar, Philippines, Thailand and Vietnam. Our Asian network also includes regional desks focused on Japan and South Asia.