Technology, Media & Telecommunications

Cybersecurity Bill Tabled in Parliament – Key Amendments Made to Earlier Draft Bill

Introduction

On 8 January 2018, the Cybersecurity Bill ("**the Bill**") was introduced in the first Parliament sitting of 2018.

Earlier, between 10 July 2017 and 24 August 2017, the Ministry of Communications and Information ("**MCI**") and the Cyber Security Agency of Singapore ("**CSA**") invited the public to provide feedback on the draft Cybersecurity Bill ("**Draft Bill**"). Please see here for our earlier Client Update on the public consultation. On 13 November 2017, the MCI and CSA published its report on the feedback received from the public consultation ("**Report**").

The Bill takes into account the feedback received from the public consultation. This Update highlights the main changes between the Draft Bill and the Bill, and provides our preliminary comments on the same.

Main Changes

The following are the main changes which have been made to the Draft Bill, many of which are in response to the feedback received from the public consultation.

Critical Information Infrastructure owner

(a) Definition of Owner of a Critical Information Infrastructure

The Bill now defines the owner of a Critical Information Infrastructure ("**CII**") as the legal owner of the CII and, where the CII is jointly owned by more than one person, includes every joint owner. As a corollary, computer systems in the supply chain supporting the operations of a CII will not be designated as CIIs and therefore third-party vendors will not be considered as owners of CIIs. This is in response to comments received from the public consultation that there could be examples where more than one party could fulfil the definition of a CII owner for the same CII under the Draft Bill, for example in outsourced business operations.

Additionally, the Bill allows for a person who receives a notice from the Commissioner of Cybersecurity ("**Commissioner**") designating his computer or computer system to be a CII to request the Commissioner to amend the notice and send the amended notice to another person upon showing proof that:

(i) the person is not able to comply with the duties of a CII owner because the person has neither effective control over the operations of the computer or computer system, nor the ability or right to carry out changes to the computer or computer system; and

(ii) another person has effective control over the operations of the computer or computer system and the ability and right to carry out changes to the computer or computer system.

If the Commissioner is satisfied that the above conditions are met, the Commissioner may send an amended notice to the person mentioned in (ii) above instead who would then be subject to all the duties of a CII owner. Further, where a notice is amended and sent to the person mentioned in (ii) above, and that person ceases to have the control, ability and right to the CII, then the owner of the CII must notify the Commissioner of this without delay.

(b) Reporting on change in ownership

Where there is a change in ownership of CII, the CII owner will be required to inform the Commissioner of the change in ownership not later than 7 days after the date of that change in ownership. This is consistent with the announcement made by the MCI and CSA in the Report, in which they took into account feedback on the impracticality of requiring CII owners to inform the Commissioner of any intended change in ownership of the CII not later than 90 days before the date of the intended change in ownership.

(c) Duty to report cybersecurity incident in respect of CII

Previously under the Draft Bill, there were concerns that the requirement for CII owners to establish mechanisms and processes as may be necessary in order to detect any cybersecurity threats in respect of CII might be overly onerous, given the wide range of cybersecurity threats and the difficulties in detecting them all.

Under the Bill, CII owners are required to establish mechanisms and processes for the purpose of detecting cybersecurity threats and incidents in respect of the CII as set out in any applicable code of practice.

(d) Audit and risk assessment

Under the Bill, CII owners are required to conduct audits at least once every two years (or such higher frequency as may be directed by the Commissioner), and to conduct risk assessments at least once a year.

Previously, under the Draft Bill, the requirement to conduct audits and risk assessments was at least once every three years.

Disclosure of information to the Commissioner

(a) Rules of Professional Conduct

Under the earlier Draft Bill, the Commissioner was empowered to request for certain information from an owner of a computer or computer systems, or a CII owner, except in a scenario where doing so would constitute a breach of written law by that owner.

Presently under the Bill, a person (whether an owner of a computer or computer system, or a CII owner) who is requested by the Commissioner to provide such information is not obliged to do so if the information is subject to any right, privilege, immunity, obligation or limitation imposed by any rules of professional conduct in relation to the disclosure of such information.

In this regard, the Bill makes clear that a person's right to legal professional privilege will still be protected. A person will not be obliged to disclose information to the Commissioner if such information is subject to legal professional privilege.

(b) Contractual obligations

On the contrary, under the Bill, a CII owner will be required to disclose to the Commissioner any information relating to the CII upon the latter's request, notwithstanding that doing so may amount to a breach of the former's obligations under other contracts. The Bill specifically states that the CII owner's performance of a contractual obligation would *not* be an excuse for not disclosing the information. This obligation is reinforced by section 10(4) of the Bill, whereby a CII owner would not be treated as breaching its contractual obligation if the act of disclosure to the Commissioner was made with reasonable care and in good faith for the purpose of complying with the notice issued by the Commissioner.

Therefore, insofar as the Bill is concerned, it is crystal clear that a CII owner will not be able to rely on contractual obligations (e.g. Confidentiality obligations in a non-disclosure agreement) when requested by the Commissioner. Should the other party to the contract subsequently wish to take action against the CII owner, section 10(4) of the Bill provides a defence (subject to the conditions in that provision) to the CII owner as to why it should not be treated as being in breach of its obligations under the contract.

Licensing framework for cybersecurity service providers

As announced by the MCI and CSA in the Report, the licensing regime is narrower under the Bill. Under the earlier draft Bill, vendors providing both "investigative" and "non-investigative" cybersecurity would require a license. These include organisations and their employees which provide penetration testing services and managed security operations centres ("**SOCs**") monitoring services.

Now, the Bill only requires vendors which provide penetration testing services and/or managed SOCs monitoring services to be licensed. These include resellers of such services. The distinction between "investigative" and "non-investigative" types of licensable services has also been removed.

As a result, there is no longer a requirement for individual cybersecurity professional to be licensed; licensing will be done at the company level. The licensing obligations is therefore less onerous for cybersecurity organisations, as it means that a licensable cybersecurity service provider is required to apply for one license for itself instead of its respective cybersecurity employees having to apply for individual licenses. Nevertheless, to improve and uphold the professional standards of cybersecurity professionals, the authorities have indicated that they will seek to establish voluntary accreditation regimes to improve the standing and quality of cybersecurity professionals in Singapore.

Additionally, the duration of service record keeping has been reduced from five years to three years.

As to the implementation timeline, the Bill provides for licensable service providers to apply for a license within six months from the date of the commencement of the Cybersecurity Act.

Related amendments to the Computer Misuse and Cybersecurity Act

The Bill makes consequential and related amendments to certain other acts. Specifically, the provision in relation to emergency cybersecurity measures and requirements in the Computer Misuse and Cybersecurity Act will be repealed and re-enacted with slight modification under the Bill. The Computer Misuse and Cybersecurity Act will also be renamed to the Computer Misuse Act.

Closing Comments

As noted, many of the changes to the Bill were made in response to the feedback received from the public consultation. Therefore, businesses and industry players should welcome the changes in the Bill to clarify that only systems which have been explicitly designated by the Commissioner will be considered CII.

It may be useful to note that the owner of a CII will not be obliged to furnish information that is protected by any law or professional conduct rules. As mentioned above, a CII owner would accordingly not be obliged to disclose information which is subject to legal professional privilege. However, performance of a contractual obligation will not be an excuse for CII owners when asked to hand over information to the authorities.

Also, it is expected that the relevant authorities will issue more specific codes of practice to stipulate, amongst others, the mechanisms and processes for the purpose of detecting cybersecurity threats and incidents that CII owners are required to establish. The codes of practice/guidelines will provide more guidance to the relevant businesses on the actions that they must take to comply with the Cybersecurity Act.

The amendments to the Bill indicate that the Government is seeking to take a balanced approach – while the Government takes cybersecurity threats and incidents very seriously and recognises the need to establish pre-emptive measures to safeguard our essential services, it has also sought to limit the scope of the application and to ensure that it does not impose an unreasonable burden on the relevant businesses or discourage them from operating certain services in Singapore.

The Cybersecurity Act, when passed, will be a key piece of legislation for potential CII owners, industry associations and cybersecurity professionals to take note of.

For further enquiries or discussion, please feel free to contact our team below.

Contacts

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

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

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

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

Lionel Tan
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

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

Benjamin Cheong
Partner, Technology, Media & Telecommunications
Rajah & Tann Singapore LLP

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

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

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 7304 0763 / +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 +632 894 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

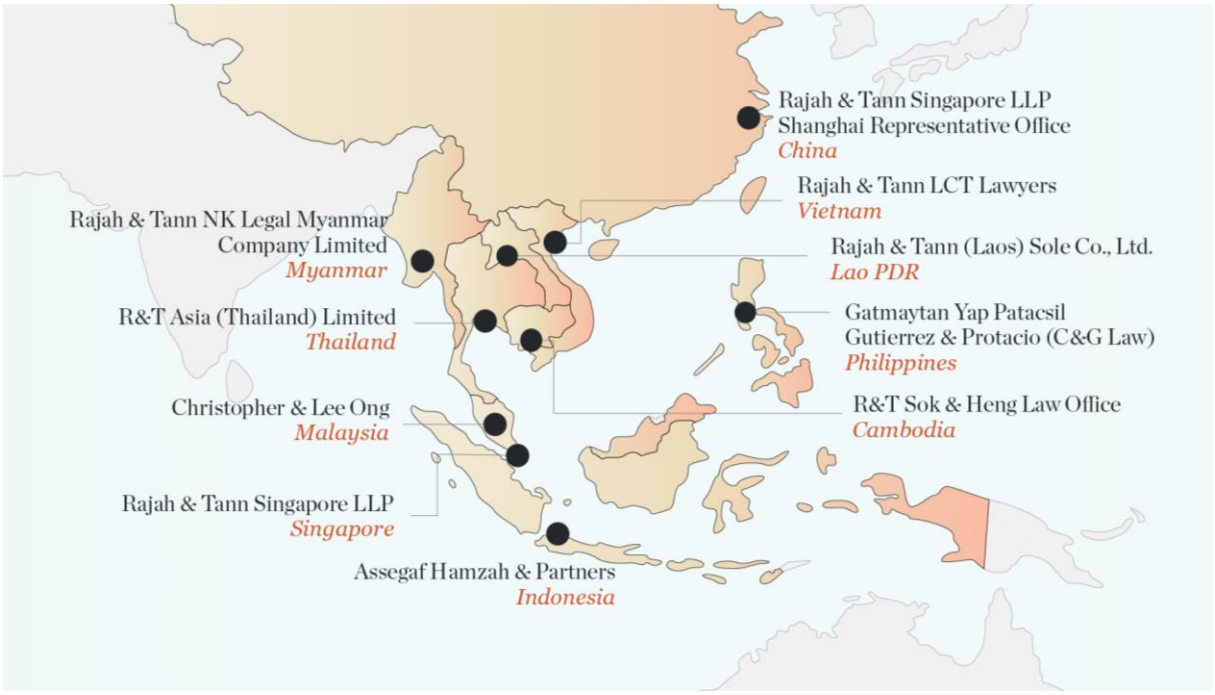
RAJAH & TANN LCT LAWYERS | *Vietnam*

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.