Technology, Media & Telecommunications

Tackling New Challenges in Cybersecurity – CSA Issues Public Consultation on Draft Cybersecurity (Amendment) Bill

Introduction

The cybersecurity landscape is constantly shifting, with new threat factors emerging at an ever-accelerating rate. Combined with the increasing connectivity and data storage needs arising from Singapore's rapid digitalisation, it has become a priority to keep pace with changing cybersecurity needs.

To keep Singapore's legislative framework up to date, the Cybersecurity Agency of Singapore ("**CSA**") has introduced the draft Cybersecurity (Amendment) Bill ("**Draft Bill**"). The Cybersecurity Act, which came into force in August 2018, is the statute that governs the oversight and maintenance of national cybersecurity in Singapore. The Draft Bill seeks to update the Cybersecurity Act to ensure that Singapore's cybersecurity laws remain fit-for-purpose, and capable of addressing the emerging challenges, including the growing importance of – and our increasing dependence on – digital infrastructure such as cloud storage services and data centres.

Among other changes, the Draft Bill seeks to:

- **Update existing laws pertaining to the protection of Critical Information Infrastructure ("CII")**, and to continue to maintain a high standard of protection for these systems.

- **Extend the Commissioner of Cybersecurity's ("Commissioner") oversight**, so that CSA can do more to safeguard nationally important computer systems and support entities of special cybersecurity interest.

- **Enable a greater situational awareness of the cybersecurity threats** to foundational digital infrastructure, **and the power to mandate baseline cybersecurity standards** for these foundational digital infrastructure.

In particular, the Draft Bill recognises the importance of entities in charge of key digital infrastructure other than CIIs, and seeks to safeguard these entities and prevent widespread service disruption by increasing oversight over their cybersecurity and requiring compliance with minimum standards. Such entities may include cloud service providers and data centre operators.

Technology, Media & Telecommunications

While the full extent of these new obligations has yet to be spelt out, seeing the wide scope of obligations currently imposed on CIIs (such as banks, telecommunications companies and energy companies), which includes the prompt reporting of cyber attacks and the implementation of specified cyber safety standards, it may be expected that the eventual enforcement regime covering cloud service providers, data centre operators, and other entities under the Draft Bill will be of similar scope. This means that the amendments may have a potentially deep impact on the duties and requirements that these entities must comply with.

CSA has issued a public consultation seeking views on the Draft Bill. The public consultation is open from 15 December 2023 to 15 January 2024. Stakeholders and industry players should consider the proposed changes and provide feedback on any issues and concerns they may have.

This Update provides a summary of the Draft Bill and highlights the key proposed amendments.

Purpose

CSA has stated that the broad purpose of the amendments to the Cybersecurity Act as contained in the Draft Bill is to:

- **Keep pace with developments in technology and industry practices** – To ensure that the Cybersecurity Act remains relevant as technology and business models evolve.

- **Look beyond CII to ensure the cybersecurity of other important systems and infrastructure** – To extend the coverage of the Cybersecurity Act to address the broader ecosystem as the increased adoption of digital technologies has also increased exposure to growing cyber threats.

- **Respond to evolving cybersecurity challenges** – To update regulations to ensure that the Commissioner has early and timely information of the cybersecurity vulnerabilities, threats, and incidents that affect CIIs, and other identified systems and infrastructure.

Critical Information Infrastructure

CII are computers or computer systems that are necessary for the continuous delivery of essential services in Singapore, and their cybersecurity is safeguarded under Part 3 of the Cybersecurity Act. The Draft Bill seeks to facilitate advances in virtual computing and the availability of a wider and more sophisticated range of computing services (such as cloud computing), as well as to improve operationalisation of the provisions governing CII cybersecurity.

Technology, Media & Telecommunications

Computing vendors

Under the current Part 3 of the Cybersecurity Act, the duties in relation to the CII are imposed on the owners of the CII at the first instance, as providers of essential services tend to own and control the CII. The Draft Bill includes a new Part 3A to facilitate the use of virtual computers or the use of vendors that can meet specific computing needs ("**computing vendors**") to improve a provider's ability to provide essential services.

Part 3A will allow the Commissioner to subject such providers of essential services to duties including:

- Provide the Commissioner with information on the non-provider-owned CII;
- Comply with relevant codes of practice, standards of performance or written directions;
- Notify the Commissioner of any change in the beneficial or legal ownership of the non-provider-owned CII;
- Notify the Commissioner of any prescribed cybersecurity incident involving the non-provider-owned CII;
- Cause regular audits of the compliance of the non-provider-owned CII with the Cybersecurity Act, codes of practice and standards of performance;
- Cause regular risk assessments of the non-provider-owned CII; and
- Participate in cybersecurity exercises.

Under the proposed Part 3A, the provider of essential services will be required to obtain legally binding commitments from their computing vendor to ensure that the provider of the essential service is able to discharge its duties under the Cybersecurity Act. In the event that the provider of the essential service fails to obtain the required commitments, the Commissioner may order the provider of the essential service to cease the use of the non-provider-owned CII.

Incident reporting

The Draft Bill proposes to expand the types of cybersecurity incidents regarding provider-owned CII to be reported to the Commissioner to include:

- Prescribed cybersecurity incidents in respect of any other computer or computer system under the owner's control that does not fall within Section 14(1)(b) of the Cybersecurity Act; and

- Prescribed cybersecurity incidents in respect of any computers or computer systems under the control of a supplier to the owner that is interconnected or communicates with the provider-owned CII.

The Draft Bill also proposes that persons with duties under Part 3A be required to report the following:

- Prescribed cybersecurity incidents in respect of the non-provider-owned CII;
- Prescribed cybersecurity incidents in respect of any computer or computer system under the owner's control, or the provider's control, that is interconnected with or that communicates with the non-provider-owned CII;
- Prescribed cybersecurity incidents in respect of any other computer or computer system under the provider of essential services' control that does not fall within the prior requirement; and
- Any other type of cybersecurity incidents in respect of the non-provider-owned CII that the Commissioner has specified by written direction.

Other amendments

The Draft Bill proposes to make other updates to the provisions governing provider-owned CII, including:

- Allowing computers or computer systems to be designated provider-owned CII even if the computer system is located wholly overseas;
- Allowing the Commissioner to grant a time extension to a designation for a provider-owned CII and for a provider of essential services responsible for the non-provider-owned CII under the new Part 3A;
- Granting the Commissioner the power to authorise the conduct of on-site inspections of provider-owned CII located in Singapore; and
- Allowing the Commissioner to grant time extensions to persons with duties under Part 3 and Part 3A.

Oversight of Other Important Systems and Infrastructure

Apart from CIIs, CSA has recognised that there are other nationally important computer systems that face heightened risks during crucial periods, as well as entities of special cybersecurity interest. The Draft Bill thus proposes to extend the Commissioner's oversight over these entities, to enhance CSA's

situational awareness of prescribed cybersecurity threats and incidents targeting such entities, and to ensure that an adequate level of cybersecurity is met.

Designation

The Draft Bill empowers the Minister or Commissioner to designate the following categories of entities:

- **Foundational digital infrastructure ("FDI") services** – These are services that promote the availability, latency, throughput or security of digital services.

- **Major FDI service providers** – These are FDI service providers that provide 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.

- **Entities of special cybersecurity interest ("ESCIs")** – These 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.

- **Systems of temporary cybersecurity concern ("STCC")** – These are computers or computer systems (located wholly or partly in Singapore) where 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. A STCC may be designated as such for a period of no more than one year (although this may be extended).

Duties

Once designated, a major FDI service provider, ESCI or STCC would be subject to several duties, including the following:

- **Provision of information** – A major FDI service provider, ESCI or STCC will be required to provide the Commissioner with information related to their cybersecurity.

- **Codes of practice** – A major FDI service provider, ESCI or STCC must comply with such codes of practice, standards of performance or written directions in relation to STCC as may be issued by the Commissioner.

- **Notification of incidents** – A major FDI service provider, ESCI or STCC will be required to notify the Commissioner of any prescribed cybersecurity incident.

- FDI – Incidents that result in a disruption or degradation to the continuous delivery of the FDI service, or incidents that have a significant impact on the major FDI provider's business operations in Singapore.

- ESCI – Incidents that result in a breach of the availability, confidentiality or integrity of the ESCI's data, or incidents that have a significant impact on the business operations of the ESCI .

- STCC – Prescribed cybersecurity incidents in respect of: (a) the STCC; (b) any computer or computer system under the owner's control, that is interconnected with or that communicates with the STCC; and (c) any computer or computer system under the control of a supplier to the owner that is interconnected with or communicates with the STCC.

Other Amendments

Under Part 5 of the Cybersecurity Act, persons engaging in the business of providing licensable cybersecurity services must have a cybersecurity service provider's licence. The grant or renewal of a licence may be subject to such conditions as the Licensing Officer thinks fit to impose.

To facilitate the operationalising of Part 5, the Draft Bill proposes to amend the Cybersecurity Act to include monitoring powers for Licensing Officers. These include powers of entry and inspection.

Concluding Words

The impact of the proposed amendments in the Draft Bill is potentially wide-reaching, allowing for the designation of new categories of entities falling within the scope of the Cybersecurity Act, and for the imposition of a series of duties over such entities. This would include codes of conduct and standards of performance that have yet to be determined, though CSA has stated that it will work with industry stakeholders to co-create the applicable standards and lean on the industry's experience and best practices.

Stakeholders such as cloud service providers and data centre operators should assess whether they fall within the scope of the Draft Bill, and if so, how the proposed duties will affect their operations, and whether there may be any issues or concerns in terms of compliance. CSA invites members of the public and stakeholders to provide their feedback by 5pm on 15 January 2024.

Parties looking to consult on feedback that they wish to provide should feel free to contact our Technology, Media & Telecommunications team below. As practitioners specialising in the areas where technology and law intersect, and with experience in issues of cybersecurity and compliance, the team is well placed to assist with the crafting of responses to the consultation. In addition, the team at Rajah

Technology, Media & Telecommunications

& Tann Cybersecurity is able to advise on cybersecurity and the assessment of your organisation's compliance framework, which will be key in ensuring compliance with any cybersecurity requirements which may be imposed under the proposed Draft Bill.

Click on the following links for more information (available on the CSA Portal at www.csa.gov.sg):

- Press release titled "Public Consultation on the Cybersecurity (Amendment) Bill"
- Public Consultation Document
- Draft Cybersecurity (Amendment) Bill

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

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

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) 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

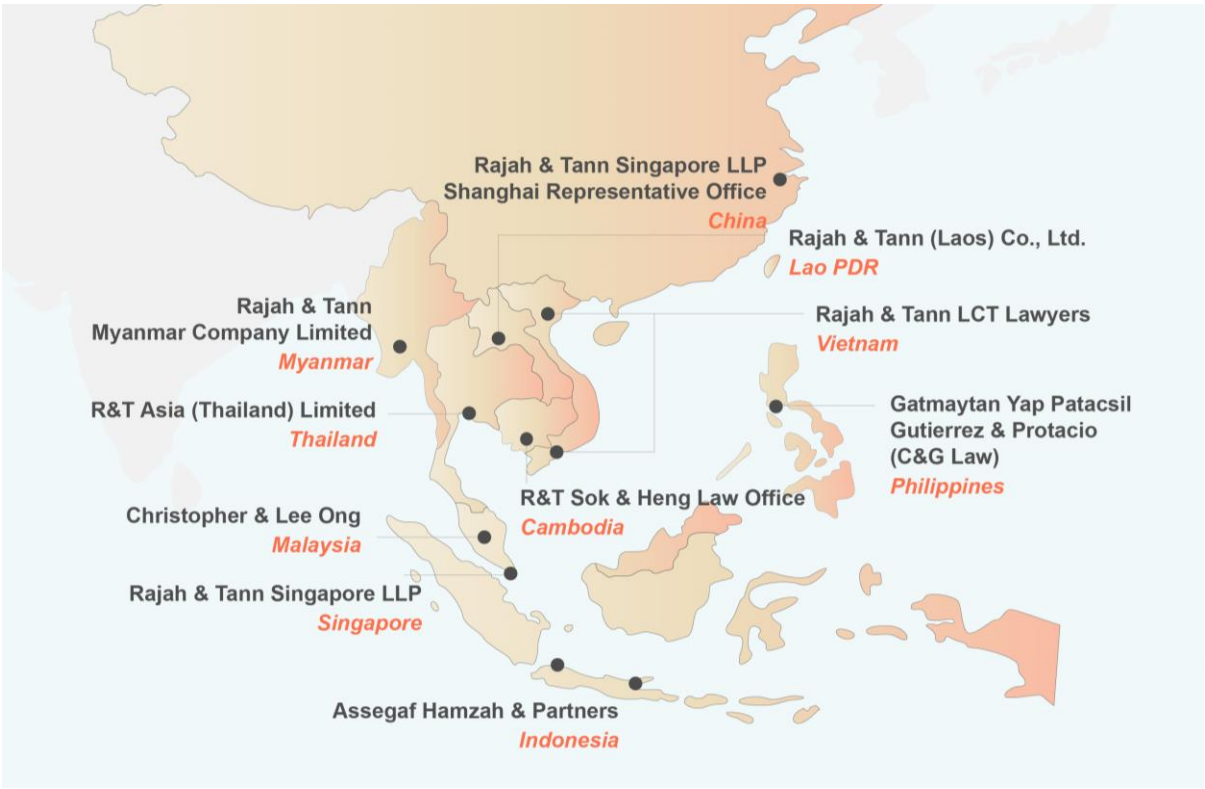
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

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.