Technology, Media and Telecommunications & Data Protection

Upcoming Cyber Security Act: What You Need To Know

Introduction

On 25 March 2024, the long-awaited Cyber Security Bill 2024 ("**Bill**") was tabled in Parliament by the Minister of Digital, Gobind Singh Deo. The Bill seeks to introduce an overarching cyber security legislation to enhance national cyber security.

This Update aims to provide a brief overview of the key principles of the Bill and how to stay ahead of the upcoming regulatory changes.

Background

By way of background, there is currently no single legislation in respect of cyber security in Malaysia, though there are existing laws relating to cyber security in separate pieces of legislation, e.g. Computer Crimes Act 1997, Communications and Multimedia Act 1998, Personal Data Protection Act 2010, Penal Code, etc.

For years, the Malaysian Government has called for an overarching cyber security legislation, acknowledging the issues and challenges associated with cyber security threats.

- In October 2020, the Malaysian Government had released the Malaysia Cyber Security Strategy (2020-2024) which introduced five strategic pillars for the management of and preparedness for cyber security threats in Malaysia, one of which included the need for enhancement of existing cyber security laws and introduction of new cyber security laws.[1]

- In August 2023, Fahmi Fadzil, the then Minister of Communications and Digital (now the Minister of Communications), announced that a cyber security bill was being drafted[2] and is expected to be tabled in the Malaysian Parliament by early 2024.[3]

- On 24 November 2023, a dialogue session in relation to the rationale and contents of the draft cyber security bill ("**Dialogue Session**") was held by the National Cyber Security Agency ("**NACSA**") to brief and solicit feedback from the relevant industry stakeholders.

[1] https://asset.mkn.gov.my/wp-content/uploads/2020/10/MalaysiaCyberSecurityStrategy2020-2024.pdf (page 28/91, 44-48/91)
[2] https://www.kkd.gov.my/images/pdf/ucapan2023/230801_ybm_keynote_public_sector_day.pdf (page 6/7)
[3] https://www.thestar.com.my/news/nation/2023/08/15/cybersecurity-bill-to-be-tabled-by-early-next-year-says-fahmi

- In late November 2023, the Malaysian Cabinet approved the drafting of the cyber security bill in principle, which was reportedly completed pending feedback from various ministries.[4]

The sequence of events above led to the tabling of the Bill.

Key Principles of the Bill

If and when the Bill comes into force (the "**Act**"), it is expected to serve as the overarching cyber security legislation, to be read together with existing laws relating to cyber security in Malaysia, resulting in a more comprehensive and encompassing legislative framework to combat cybercrimes.

This also means that businesses and sectors which are subject to the Act are expected to put in place additional measures to comply with the requirements under the Act.

Set out below is a summary of the key principles of the Bill.

(a) The Act binds the Government

Pursuant to the Bill, the Act shall bind the Federal Government and State Governments, but nothing in the Act shall render the Federal Government and State Governments liable to prosecution for any offence under the Act.

This is a departure from the existing Personal Data Protection Act 2010 which currently does not apply to the Federal Government and State Governments.

(b) Extra-territorial application

The Bill further proposes that the Act shall have extraterritorial application if an offence is committed under the Act in relation to a national critical information infrastructure ("**NCII**", defined below) that is wholly or partly in Malaysia.

It was understood from the Dialogue Session that the rationale for the extra-territorial application of the Act is due to the borderless nature of technology. This means that foreign businesses may be caught within the purview of the Act where it pertains to NCIIs that are wholly or partly in Malaysia.

(c) National Critical Information Infrastructure

The term "national critical information infrastructure" is defined under the Bill as a computer or computer system which the disruption or destruction thereof would have a detrimental impact on the delivery of any service essential to the security, defence, foreign relations, economy, public health, public safety or public order of Malaysia, or on the ability of the Federal Government or any of the State Governments to carry out its functions effectively.

[4] https://www.nst.com.my/news/nation/2023/11/984004/cybersecurity-bill-be-tabled-parliament-early-next-year

The Bill further specifies the following as **NCII sectors**:

- government sector;
- banking and finance sector;
- transportation sector;
- defence and national security sector;
- information, communication and digital sector;
- healthcare services;
- water sewerage and waste management sector;
- energy sector;
- agriculture and plantation sector;
- trade, industry and economy sector; and
- science, technology and innovation sector.

Businesses in the NCII sectors above, if designated as an NCII entity under the Act ("**NCII Entities**"), may therefore be required to fulfil certain duties under the Act.

(d) Establishment of the National Cyber Security Committee

The Act will establish the National Cyber Security Committee ("**Committee**"), comprising various ministerial stakeholders, including the Prime Minister, Minister of Finance, Minister of Foreign Affairs, Minister of Defence, Minister of Home Affairs, Minister of Communications, Inspector General of Police, etc., as well as no more than two other persons of standing and experience in cyber security.

The Committee is chaired by the Prime Minister and assisted by the Chief Executive of the NACSA ("**Chief Executive**") who will act as the secretary to the Committee.

It is anticipated that the Committee will assume the leading role in the formulation and implementation of policies relating to national cyber security, be given the powers to provide directions to the Chief Executive and oversee the effective implementation of the Act.

(e) Reinforces NACSA as the lead cyber security agency in Malaysia

NACSA, being the federal agency for cyber security matters, currently has limited regulatory purview and enforcement powers in relation to cyber security matters. The Bill proposes to reinforce NACSA as the lead cyber security agency in Malaysia by specifying its functions to include, among others, the administration of the Act and maintenance of a national cyber security system known as the "National Cyber Coordination and Command Centre System" for the purpose of dealing with cyber security threats and cyber security incidents.

The Bill also makes it the duty of the Chief Executive to advise the Committee, implement policies relating to cyber security, collect and disseminate information based on information provided by NCII Sector Leads (defined below) and NCII Entities, and issue directives to NCII Sector Leads and NCII Entities on matters relating to cyber security in Malaysia.

The Bill further proposes to clothe NACSA with the regulatory and enforcement powers necessary to investigate national cyber security matters, threats and incidents, e.g. directing a person to provide information and documents, conducting search and seizure, obtaining access to computerised data, etc.

(f) Establish a cyber security governance framework

The Bill proposes that the Minister may, upon the recommendation of the Chief Executive, designate one or more government entity or person as NCII sector leads ("**NCII Sector Leads**").

NCII Sector Leads will, in turn, be responsible for, among others, designating NCII Entities within their respective sectors, preparing a code of practice for their respective sectors, and implementing the decisions of the Committee and directives issued under the Act.

(g) Duties of NCII Entities

The Bill proposes that NCII Entities be subject to various duties under the Act, including:

- implementing the measures, standards and processes as specified in the code of practice issued by the respective NCII Sector Leads;
- conducting cyber security audits and risk assessments;
- notifying the Chief Executive and its NCII Sector Lead(s) in the event of any cyber security incident;
- carrying out cyber security exercise as directed by the Chief Executive; and
- complying with various directives issued under the Act.

(h) Establish a licensing regime for cyber security service providers

The Bill proposes the establishment of a new licensing regime for cyber security service providers whereby they should be duly licensed in order to provide cyber security services and must comply with related licence conditions.

While the Bill does not specify the types of cyber security services that are subject to the licensing regime, we understand based on the Dialogue Session that this will likely apply to service providers that provide services to safeguard information and communications technology device of another person (e.g. penetration testing providers and security operation centres).

Staying Ahead of the Upcoming Regulatory Changes

Considering the proposed governance structure under the Bill, it is pertinent to note that the Act will likely only serve as an umbrella legislation and a framework for the Malaysian Government to coordinate activities between the ministries and industry stakeholders, and that the cyber security requirements will be tailored for each NCII sector in the form of codes of practice which are to be issued by the respective NCII Sector Leads.

That said, the tabling of this Bill is a significant step by the Malaysian Government to ensure the preparedness of the legal and regulatory landscape in Malaysia in responding to cyber security threats

and to align with various national policy commitments in managing the challenges associated with the increasing adoption and use of technologies.

We expect to see robust, comprehensive and far-reaching legislative developments in the area of cyber security in the coming months, involving several ministries as well as NCII Sector Leads in various NCII business sectors. As such, all relevant businesses and stakeholders are advised to stay abreast of these developments and take the necessary steps in preparation for the enactment of the new Act.

We trust the above provides a useful update on the latest developments in the cyber security regulatory landscape in Malaysia. Should you require any assistance or clarification in relation to the above, or any matter relating to cyber security, please feel free to contact our team members below at your convenience.

Contacts

Deepak Pillai
Head
Technology, Media & Telecommunications; Data Protection

T +603 2267 2675
M +601 2213 4674
deepak.pillai@christopherleeong.com

Intan Haryati Binti Mohd Zulkifli
Partner
Technology, Media & Telecommunications; Data Protection

T +603 2267 2674
F +603 2273 8310
intan.haryati@christopherleeong.com

Anissa Maria Anis
Partner
Technology, Media & Telecommunications; Media & Entertainment

T +603 2267 2750
M +601 2371 9129
anissa.anis@christopherleeong.com

Yong Shih Han
Partner
Technology, Media & Telecommunications; Data Protection

T +603 2267 2715
M +601 2480 8863
shih.han.yong@christopherleeong.com

Contribution Note

This Client Update is contributed by the Contact Partners listed above, with the assistance of **Lee Suke Mune** (Senior Associate, Christopher & Lee Ong) and **Yu Xin Yi** (Associate, Christopher & Lee Ong).

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

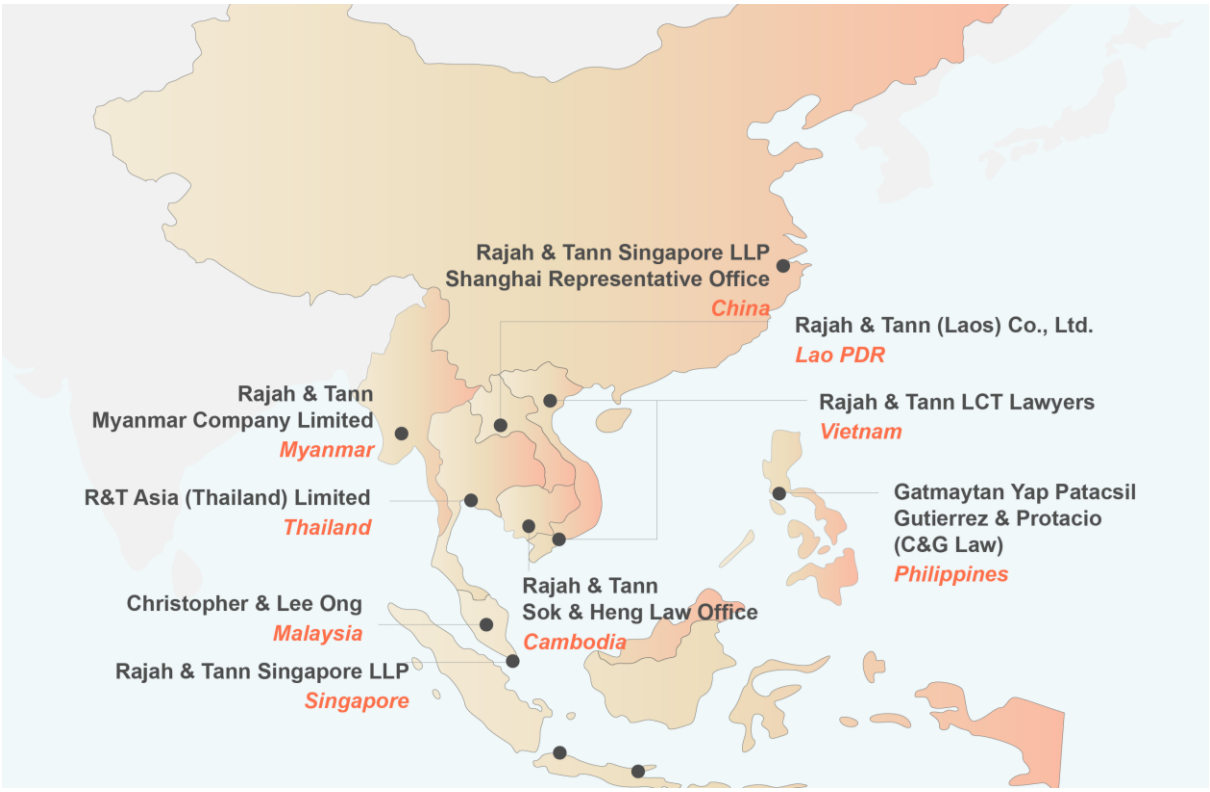
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

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



Christopher & Lee Ong is a full service Malaysian law firm with offices in Kuala Lumpur. It is strategically positioned to service clients in a range of contentious and non-contentious practice areas. The partners of Christopher & Lee Ong, who are Malaysian-qualified, have accumulated considerable experience over the years in the Malaysian market. They have a profound understanding of the local business culture and the legal system and are able to provide clients with an insightful and dynamic brand of legal advice.

Christopher & Lee Ong 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.