Technology, Media And Telecommunications & Data Protection

Coming into Force of the Cyber Security Act 2024 and the New Subsidiary Regulations

Introduction

In our previous Update and Snapshot Deck, we provided a brief overview of the regulatory structure and key requirements introduced by the Cyber Security Act 2024 (Act 854) ("**CSA**") which was gazetted in the Federal Gazette on 26 June 2024 but had then yet to come into force.

This Update aims to (i) set out the new date of coming into force of the CSA, (ii) offer a brief overview on the new subsidiary regulations which will complement the implementation and enforcement of the CSA, and (iii) provide some pointers on what businesses may expect to happen next, as well as how to prepare for developments in respect of the CSA.

When will the CSA come into force?

The Malaysian Government has appointed ***26 August 2024*** as the date of coming into force of the CSA.[1]

It remains to be seen whether any grace period will be given before the National Cyber Security Agency ("**NACSA**") enforces the CSA against any person designated as an NCII entity under the CSA ("**NCII Entity**") or any cyber security service provider that does not comply with the CSA.

However, businesses may wish to note the Chief Executive of NACSA ("**Chief Executive**") indicated in a conference in July 2024 that while the CSA is not intended to be a punitive legislation, enforcement actions will be pursued against those who wilfully disregard or refuse to comply with the CSA or any directions issued by NACSA under the CSA.

New Subsidiary Regulations under the CSA

The Malaysian Government has issued four subsidiary regulations to complement and operationalise the CSA effectively.

[1] Appointment of Date of Coming into Operation (P.U. (B) 334)

[I] Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024

The Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024 set out the frequency for conducting cyber security risk assessments and audits as required under the CSA:

(a) cyber security **risk assessments** to be conducted at least **once** a year; and
(b) cyber security **audits** to be conducted at least **once every two years**, or at such higher frequency as may be directed by the Chief Executive.

[II] Cyber Security (Notification of Cyber Security Incident) Regulations 2024

The Cyber Security (Notification of Cyber Security Incident) Regulations 2024 provide further clarity regarding the timeline, form, and manner for the notification of cyber security incidents as required under the CSA.

	Timeline	Form	Manner
Initial notification	Within six hours from the time the incident comes to the knowledge of the NCII Entity.	Details on the authorised person, NCII Entity, NCII Sector, NCII Sector Lead, and the cyber security incident.	Any system as designated by the National Cyber Coordination and Command Centre (**NC4**) or the Chief Executive.
Subsequent notification	Within 14 days after the initial notification.	Details of the affected NCII, as well as the impact, threat actor, tactic used by the threat actor, and action taken by the NCII Entity in relation to the cyber security incident.	

[III] Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024

The Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024 ("**CSP Licensing Regulations**") provide further clarity on the scope of cyber security services which are subject to the licensing requirement under the CSA.

The licensing requirement applies to:

(a) **managed security operation centre monitoring services**, i.e. services for monitoring the level of cyber security of a computer or computer system of another person, or services for determining the measures necessary to respond to, recover from, or prevent cyber security incidents; and
(b) **penetration testing services**, i.e. services for assessing, testing, or evaluating the level of cyber security of a computer or computer system

(collectively, "**Licensable Services**").

The licensing requirement does not apply if:

(a) the Licensable Services are provided by a Government Entity;
(b) the Licensable Services are provided to a related company; or
(c) the computer or computer system in respect of which the Licensable Services are provided are located outside Malaysia.

[IV] Cyber Security (Compounding of Offences) Regulations 2024

The Cyber Security (Compounding of Offences) Regulations 2024 identify the following offences under the CSA which are compoundable by the Chief Executive:

(a) failure of a NCII Entity to provide information relating to their NCII to their NCII Sector Lead;
(b) failure to conduct and submit reports of cyber security risk assessments and audits to the Chief Executive;
(c) failure to rectify reports of cyber security risk assessments and audits, and comply with directions from the Chief Executive in respect of the cyber risk assessments and audits;
(d) failure to comply with the directions of the Chief Executive in relation to cyber security exercises; and
(e) failure of licensed cyber security service providers to keep and maintain proper records of information as required under the CSA.

What's Next?

Now that CSA has come into force, we set out below some pointers on what businesses may expect to happen next, and how to prepare for the developments in respect of the CSA.

[I] Publication of the Names of NCII Sector Leads

Under the CSA, the Minister will designate one or more NCII Sector Leads for each of identified 11 NCII Sectors, by publishing the names of the appointed NCII Sector Leads on the official website of NACSA.

These NCII Sector Leads will be responsible for designating NCII Entities within their respective sectors, preparing a code of practice for their sector and monitoring compliance of these entities with the requirements of the CSA.

[II] Designation of NCII Entities

Once the NCII Sector Leads for the NCII Sectors are appointed, they may begin to issue information requests to businesses/entities operating in their respective sectors. These requests will seek information regarding the computers or computer systems owned by these entities to determine if they should be designated as NCII Entities under the CSA.

Based on what has been done in Singapore with respect to the Singapore Cybersecurity Act 2018, we anticipate that the information requests may include details such as the description and location of the computers/computer systems, their functions, and information relating to their design.

It is also possible that NACSA will prepare a standardised information request form to ensure consistency in the information requested by NCII Sector Leads across different sectors.

[III] Preparation of Codes of Practice by NCII Sector Leads

A key component of the CSA is the sector-specific codes of practice that will be prepared by NCII Sector Leads. These codes of practice will set out the minimum cyber security measures, standards and processes that NCII Entities that must implement and comply with to protect their NCII.

The appointed NCII Sector Leads will need to develop the codes of practice for their respective sectors. We anticipate that there will be further consultation sessions conducted by NCII Sector Leads to obtain feedback from the relevant stakeholders and finalise the codes of practice.

[IV] Licence Application Process for Cyber Security Service Providers

To facilitate licence applications for the provision of Licensable Services, we expect that NACSA may issue further guidelines and may also establish a form of electronic means for businesses to apply for a cyber security service provider licence as required under the CSA and the CSP Licensing Regulations.

Conclusion

The introduction of the CSA is a significant development in our country's cybersecurity regulatory landscape to address rising cybersecurity threats as we transition towards a digitalised nation.

As such, all relevant businesses and stakeholders are advised to stay abreast of these developments, initiate steps and allocate resources in preparation for compliance with the CSA.

Businesses operating in the NCII Sectors that own or operate computers or computer systems that may potentially be considered as NCII should note that they may be designated as NCII Entities, and will therefore need to comply with the requirements of the CSA. Additionally, businesses offering Licensable Services should take note of any further guidance provided regarding the application process for the cyber security service provider licence and be ready to apply once applications are open.

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 us at your convenience.

Contacts

Deepak Pillai
Partner

D +603 2267 2675
M +6012 213 4674
deepak.pillai@christopherleeong.com

Intan Haryati
Partner

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

Anissa Maria Anis
Partner

D +603 2267 2750
M +6012 371 9129
anissa.anis@christopherleeong.com

Yong Shih Han
Partner

D +603 2267 2715
M +6012 480 8863
shih.han.yong@christopherleeong.com

Contribution Note

This Legal Update is contributed by the Contact Partners listed above, with the assistance of **Lee Suke Mune** (Senior Associate, Christopher & Lee Ong) and **Yeap Yee Lin** (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

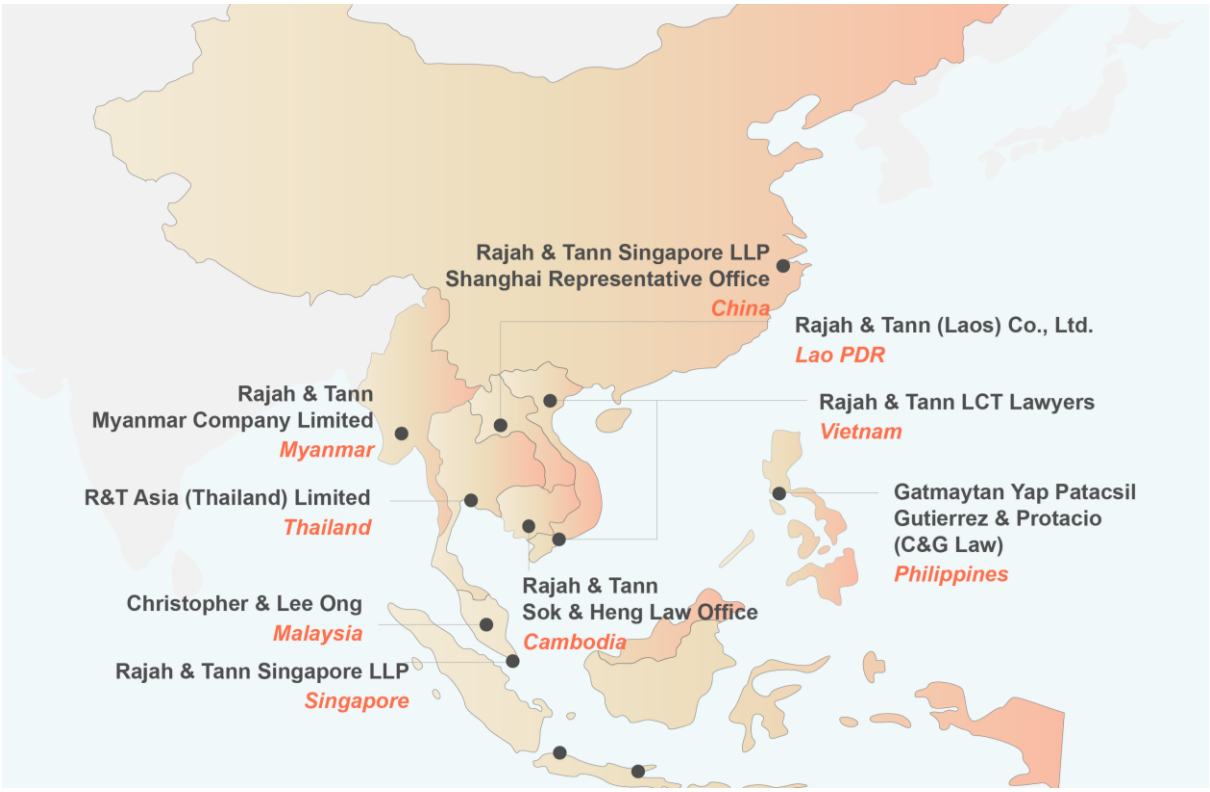
RAJAH & TANN | *Thailand*
R&T Asia (Thailand) Limited
T +66 2 656 1991
F +66 2 656 0833
th.rajahtannasia.com

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 (CLO) is a full service Malaysian law firm based in Kuala Lumpur. It is strategically positioned to service clients in a range of contentious and non-contentious practice areas. The partners of CLO, 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.

CLO 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.

Please note also that whilst the information in this Update is correct to the best of our knowledge and belief at the time of writing, it is only intended to provide a general guide to the subject matter and should not be treated as a substitute for specific professional advice for any particular course of action as such information may not suit your specific business or operational requirements. It is to your advantage to seek legal advice for your specific situation. In this regard, you may call the lawyer you normally deal with in CLO.