SKRINE

CYBER SECURITY ACT 2024 – DATE OF COMING INTO OPERATION AND SUBSIDIARY LEGISLATION GAZETTED

23 August 2024

In exercise of the power conferred onto him by section 1(2) of the Cyber Security Act 2024 ("CSA"), the Minister has appointed 26 August 2024 as the date on which the CSA comes into operation[1]. Our previous alert highlighting the salient provisions of the CSA can be accessed here.

The following regulations under the CSA, which clarify and set out the specific requirements in relation to some of the obligations imposed by the CSA, were gazetted on 22 August 2024 and will come into operation on 26 August 2024:

- Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024 [P.U.(A) 219/2024] ("Risk Assessment and Audit Period Regulations");
- Cyber Security (Notification of Cyber Security Incident) Regulations 2024 [P.U.(A) 220/2024] ("Notification Regulations");
- Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024 [P.U.(A) 221/2024] ("Licensing Regulations"); and
- Cyber Security (Compounding of Offences) Regulations 2024 [P.U.(A) 222/2024] ("Compounding Regulations").

[1] *See P.U.(B) 334/2024.*

Regulations	Salient aspects
Risk Assessment and Audit Period Regulations	The Risk Assessment and Audit Period Regulations mandate that national critical information infrastructure ("**NCII**") entities must conduct a "cyber security risk" assessment at least once a year and carry out an audit at least once every two years or in accordance with a higher frequency as may be directed by the Chief Executive of the National Cyber Security Agency ("**Chief Executive**"). "Cyber security risk" is defined as "*the risks that a vulnerability in the cyber security of the national critical information infrastructure may be exploited by a cyber security threat or cyber security incident*".
Notification Regulations	In connection with an NCII entity's duty to notify the Chief Executive and relevant NCII sector lead of cyber security incidents pursuant to section 23 of the CSA, the Notification Regulations require the notification be made by an authorised person of the NCII entity within 6 hours from the time the cyber security incident comes to the knowledge of the NCII entity ("**Initial Notification**"). The Initial Notification must contain the following: (a) particulars of the authorised person; (b) particulars of the NCII entity concerned, and the NCII sector and sector lead to which it relates; and (c) the type and description of the incident, its severity, the date and time the incident was discovered, and the method of its discovery. The Notification Regulations also require the NCII entity to, via its authorised person, provide the Chief Executive and relevant NCII sector lead the following supplementary information within 14 days after the Initial Notification ("**Subsequent Notification**"):

	(a) particulars of the NCII affected by the cyber security incident; (b) estimated number of hosts affected by the cyber security incident; (c) particulars of the cyber security threat actor; (d) artifacts related to the cyber security incident; (e) information on any incident relating to, and the manner in which such incident relates to, the cyber security incident; (f) particulars of the tactics, techniques and procedures of the cyber security incident; (g) impact of the cyber security incident on the NCII or any computer or interconnected computer system; and (h) action taken. Both the Initial Notification and the Subsequent Notification are to be submitted through the National Cyber Coordination and Command Centre System or by any other means of communication as determined by the Chief Executive.
Licensing Regulations	The Licensing Regulations prescribe that providers of the following cyber security services are subject to the licensing obligation imposed by the CSA: (a) "*managed security operation centre monitoring services*", defined as a service for: (i) monitoring the level of cyber security of a computer or computer system of another person by acquiring, identifying or scanning information that is stored in, processed by or transmitted

	through, the computer or computer system for the purpose of identifying or detecting cyber security threats to the computer or computer system; or (ii) determining the measures necessary to respond to or recover from any cyber security incident and to prevent such cyber security incident from occurring in the future. (b) "*penetration testing service*", defined as a service for assessing, testing or evaluating the level of cyber security of a computer or computer system, by searching for vulnerabilities on, and compromising, the cyber security defences of the computer or computer system, and includes any of the following activities: (i) determining the cyber security vulnerabilities of a computer or computer system, and demonstrating how such vulnerabilities may be exploited and taken advantage of; (ii) determining or testing the organisation's ability to identify and respond to cyber security incident through simulation of attempts to penetrate the cyber security defences of the computer or computer system; (iii) identifying and measuring the cyber security vulnerabilities of a computer or computer systems, indicating vulnerabilities and preparing appropriate mitigation procedures required to eliminate vulnerabilities or to reduce vulnerabilities to an acceptable level of risk; or (iv) utilising social engineering to assess the level of vulnerability of an organisation to cyber security threats.

	However, the Licensing Regulations specify that they do not apply if: (a) the cyber security service is provided by a government entity or by a person, other than a company, to its related company; or (b) the computer or computer system in respect of which the cyber security service is provided is located outside of Malaysia. The Licensing Regulations also prescribe that applications for a licence (and for renewals) are to be submitted via electronic means to the Chief Executive, accompanied by the fees prescribed in the Schedule to the Licensing Regulations. However, the precise means of submission have not been clarified.
Compounding Regulations	The Compounding Regulations identify six offences under the CSA which are compoundable offences and set out the procedures for compounding.

For further information, please contact:

CHARMAYNE ONG POH YIN
Partner
Technology, Media and Telecommunications Practice
T +603 2081 3736
E co@skrine.com

NATALIE LIM
Partner
Technology, Media and Telecommunications Practice
T +603 2081 3894
E natalie.lim@skrine.com

JILLIAN CHIA YAN PING
Partner
Technology, Media and Telecommunications Practice
T: +603 2081 3882
E: jc@skrine.com

A proud member of international legal network, LexMundi World Ready

Welcome to **Skrine**, where legal excellence meets unwavering dedication. We are a homegrown Malaysian firm known locally and internationally as a beacon of trust and proficiency in the ever-evolving landscape of jurisprudence. Founded on the principles of **wisdom**, **fortitude** and **ingenuity** over 60 years ago, we navigate the complexities of the law with precision and insight.

Through our wide range of practice groups managed by lawyers with extensive experience, we work with our clients to achieve the results they aspire. While keeping pace with rapid development on all fronts, Skrine has remained steadfast in our commitment to champion your cause with diligence, skill, and a relentless pursuit of justice.

PRACTICE AREAS

- Banking and Finance
- Construction and Engineering
- Corporate
- Corporate Structures and Secretarial Services
- Employment
- Fraud and Asset Recovery
- Intellectual Property and TMT
- Litigation and Arbitration
- Real Estate
- Regulatory Compliance
- Restructuring and Insolvency
- Tax and Revenue

INDUSTRIES

- Aviation
- Financial Institutions
- Healthcare, Biotechnology and Pharmaceuticals
- Industrial and Manufacturing
- Insurance and Reinsurance
- Maritime and Shipping
- Oil & Gas, and Energy
- Projects and Infrastructure
- Real Estate
- Technology, Media and Telecommunications

CONTACT US

Level 8, Wisma UOA Damansara
50 Jalan Dungun, Damansara Heights, 50490 Kuala Lumpur, Malaysia

T +603 2081 3999
F +603 2094 3211
E skrine@skrine.com

www.skrine.com

OUR APPROACH

While fostering a one-to-one lawyer-client relationship is of significant importance, in instances where cases do not fit neatly into one area of law, we take advantage of the various practice groups and combine the skills of our lawyers to ensure that all relevant legal issues are addressed.

ONE-STOP CENTRE WITH DEDICATED FOREIGN DESKS

We are a One-Stop Centre for all your business legal needs to help you set up in Malaysia and hit the ground running. Beyond our borders, we understand the significance of dedicated foreign desks and currently serve five major markets including **China, Turkiye, Korean, Indian (South Asia)** and **Europe**. A key benefit is the seamless and efficient delivery of our services to multilingual nations where our lawyers are proficient in Mandarin, Turkish, Hindi and Korean.

VALUE ADDED SERVICES

We recognise that from the perspective of our clients, the day-to-day management of internal legal matters does not stop at specific cases that require external legal counsel or representation. We therefore offer a number of value-added services to keep abreast with updates in the law and ensure internal compliance. This includes our e-alerts, newsletters, in-house trainings, workshops and seminars on industry-related legal topics.

FIRM AWARDS

As a testament to the high standards we uphold, Skrine has garnered some of the top local and international awards for both legal firms and individual lawyers (a full list can be viewed at our website). We are honoured to have received some of the following:

- Chambers Asia-Pacific Leading Firm Year 2024
- Legal 500 Asia Pacific: Top Tier Firm Year 2024
- Chambers Asia-Pacific and Greater China Region Awards 2024: Malaysia Law Firm of the Year
- asialaw: Malaysia Law Firm of the Year 2023
- Global Arbitration Review (GAR): Ranked in Top 100 International Arbitration Practice 2012-2023
- IFLR 1000 2019-2022: Tier 1 Firm for Corporate/Mergers & Acquisitions, Energy, Infrastructure and Oil & Gas
- Asian Legal Business: Regional Litigation Law Firm of the Year 2022