Shearn Delamore &co.

Malaysia's Cyber Security Act 2024 Comes into Operation

Introduction

We discussed the Cyber Security Bill 2024 in our April 2024 Legal Update. The Bill has since been presented for Royal Assent and has been officially gazetted. The **Cyber Security Act 2024** ("CSA") came into force on 26 August 2024 along with the following regulations:

(a) Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024 ("Risk Assessment Regulations");

(b) Cyber Security (Notification of Cyber Security Incident) Regulations 2024 ("Notification Regulations");

(c) Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024 ("Licensing Regulations"); and

(d) Cyber Security (Compounding of Offences) Regulations 2024 ("Compound Regulations").

Will my business or organisation be subject to the new law and regulations?

Public and private entities (including private businesses) that are designated as national critical information infrastructure entities ("NCII Entities") and cyber security service providers will be expected to comply with the regulatory requirements under the CSA and the abovementioned regulations.

By way of recapitulation, entities within the following sectors may potentially be designated as NCII Entities: (i) Government; (ii) Banking and Finance; (iii) Transportation; (iv) Defence and National Security; (v) Information, Communication and Digital; (vi) Healthcare Services; (vii) Water Sewerage and Waste Management; (viii) Energy; (ix) Agriculture and Plantation; (x) Trade, Industry and Economy; and (xi) Science, Technology and Innovation.

Technology, Media & Telco Update

AUGUST 2024

Shearn Delamore & Co
7th Floor
Wisma Hamzah Kwong-Hing,
No 1, Leboh Ampang
50100, Kuala Lumpur, Malaysia
T: 603 2027 2727
F: 603 2078 5625
info@shearndelamore.com
www.shearndelamore.com
www.linkedin.com/company/shearn-delamore-&-co

Risk Assessment Regulations

The Risk Assessment Regulations prescribe the frequency at which a NCII Entity shall carry out cyber security risk assessments and audits under section 22 of the CSA. Pursuant to the Risk Assessment Regulations, a NCII Entity shall:

(a) conduct a cyber security risk assessment at least once a year; and

(b) carry out an audit at least once in every two years or at such higher frequency as may be directed by the Chief Executive of the National Cyber Security Agency ("Chief Executive") in any particular case.

The Risk Assessment Regulations define "*cyber security risks*" as the risks that a vulnerability in the cyber security of the national critical information infrastructure ("NCII") may be exploited by a cyber security threat or cyber security incident.

Please note that the cyber security risk assessment and audit shall be carried out in accordance with the CSA. This means that, among others:

(a) the cyber security risk assessment shall adhere to the codes of practice as may be prepared by the relevant NCII sector lead ("NCII Sector Lead") and the directive as may be issued by the Chief Executive; and

(b) the cyber security audit shall be carried out by an auditor approved by the Chief Executive.

Failure to conduct the cyber security risk assessment or audit in accordance with the abovementioned requirements is an offence under section 22(7) of the CSA and, if convicted, will entail a fine not exceeding RM200,000 and/or imprisonment for a term not exceeding three years.

Notification Regulations

The Notification Regulations prescribe the timelines and manner for notification of a cyber security incident to be made by the authorised person of a NCII Entity to the Chief Executive and the relevant NCII Sector Lead. As discussed in our April 2024 Legal Update, the CSA defines a cyber security incident as:

> "*an act or activity carried out on or through a computer or computer system, without lawful authority, that jeopardizes or adversely affects the cyber security of that computer or computer system or another computer or computer system*."

We summarise the timelines and procedures for making a notification, as required by the Notification Regulations, in the table below (the "CSA Notification Requirements").

These requirements, along with the necessary actions and responses, must be carefully considered and where appropriate, incorporated into a NCII Entity's cyber incident response plan, cyber legal playbook, as well as the relevant cyber security training, exercises and drills.

Where a cyber incident results in or otherwise involves personal data breach, NCII Entities shall evaluate how the CSA Notification Requirements interact with the upcoming data breach notification requirements under the **Personal Data Protection Act 2010** ("PDPA"), which are yet to come into force as at the date of this Legal Update. We recently discussed the upcoming PDPA data breach notification requirements in our July 2024 Legal Update.

NCII Entities within certain regulated sectors (e.g. the banking sector) shall also evaluate how the general CSA Notification Requirements interact with their sectoral requirements that may already require cyber incident notification to be made to the relevant sectoral regulators. This includes assessing how the general and sectoral requirements may align or conflict, and ensuring that any overlaps or discrepancies are effectively managed.

The CSA Notification Requirements are summarised as follows:

Timeline & Mode	Required Information
Immediately upon the cyber security incident coming to the knowledge of the NCII Entity ("Time of Knowledge"). **Mode:** By electronic means.	Notification that a cyber security incident has or might have occurred in respect of the NCII owned or operated by the NCII Entity.
Within 6 hours from the Time of Knowledge. **Mode**: Through the National Cyber Coordination and Command Centre System (or such other method as determined by the Chief Executive in the event of a disruption).	(a) The particulars of the authorised person of the NCII Entity. (b) The particulars of the NCII Entity concerned, the NCII sector, and NCII Sector Lead. (c) The information on the cyber security incident including: (i) the type and description of the cyber security incident; (ii) the severity of the cyber security incident; (iii) the date and time the occurrence of the cyber security incident is known; and (iv) the method of discovery of the cyber security incident.

Within 14 days after the initial notification made immediately at the Time of Knowledge. **Mode**: Through the National Cyber Coordination and Command Centre System (or such other method as determined by the Chief Executive in the event of a disruption).	(a) The particulars of the NCII affected by the cyber security incident. (b) The estimated number of hosts affected by the cyber security incident. (c) The particulars of the cyber security threat actor. (d) The artifacts related to the cyber security incident. (e) The information on any incident relating to, and the manner in which such incident relates to, the cyber security incident. (f) The particulars of the tactics, techniques and procedures of the cyber security incident. (g) The impact of the cyber security incident on the NCII or any computer or interconnected computer system. (h) The action taken.
From time to time. **Mode**: Not specified.	Further updates on the cyber security incident as the Chief Executive may require.

Pursuant to section 23(2) of the CSA, it is an offence for any NCII Entity to fail to notify the Chief Executive and its NCII Sector Lead of such information in accordance with the CSA Notification Requirements, and such offence is punishable by a fine not exceeding RM500,000 and/or imprisonment for a term not exceeding 10 years.

Licensing Regulations

As discussed in our April 2024 Legal Update, the CSA provides for the licensing of cyber security service providers, but the types of services constituting "*cyber security services*" were unclear back then.

The Licensing Regulations now offer better clarity in this regard: unless any of the prescribed exceptions applies, providers of (i) managed security operation centre monitoring service and (ii) penetration testing service will have to be licensed. The definitions of these cyber security services are set out below.

Managed Security Operation Centre Monitoring Service
"Managed security operation centre monitoring service" is a service for: *(a) 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

(b) 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.

Based on the above definition, it would appear that service providers that offer assistance with responding to cyber incidents will also be considered as providing "*managed security operation centre monitoring service*" even if they do not provide monitoring services.

Penetration Testing Service

"Penetration testing service" is 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:

(a) determining the cyber security vulnerabilities of a computer or computer system, and demonstrating how such vulnerabilities may be exploited and taken advantage of;

(b) 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;

(c) identifying and measuring the cyber security vulnerabilities of a computer or computer system, indicating vulnerabilities and preparing appropriate mitigation procedures required to eliminate vulnerabilities or to reduce vulnerabilities to an acceptable level of risk; or

(d) utilising social engineering to assess the level of vulnerability of an organisation to cyber security threats.

Generally, an application for a licence to provide cyber security service and the renewal thereof shall be made by electronic means with payment of RM400 if the service provider is an individual, or RM1,000 if the service provider is a company, limited liability partnership, firm, society or other body of persons.

Providing any of the abovementioned cyber security services without a licence is an offence under section 27(5) of the CSA and, if convicted, will entail a fine not exceeding RM500,000 and/or imprisonment for a term not exceeding 10 years.

Compound Regulations

The Compound Regulations provide that the offences under sections 20(6), 20(7), 22(7), 22(8), 24(4), and 32(3) of the CSA are compoundable offences which may be compounded with the written consent of the Public Prosecutor.

Conclusion

Businesses are advised to take proactive steps in implementing necessary measures required by the CSA and the above regulations to ensure compliance.

Businesses and organisations operating within the NCII sectors are also advised to stay informed about developments relevant to their sectors, particularly with regard to the appointment of NCII Sector Leads, designation of NCII Entities, and the issuance of codes of practice and directives.

For further enquiries, please contact:

Janet Toh Yoong San
Head, Personal Data Protection & Privacy
Co-Head, Technology, Media & Telco
E: janet.toh@shearndelamore.com
T: +603 2027 2978

Boo Cheng Xuan
Associate, Personal Data Protection & Privacy
Associate, Technology, Media & Telco
E: boo.chengxuan@shearndelamore.com
T: +603 2027 2662