LHAG

SPECIAL ALERT!

Cyber Data Privacy

Arissa Ahrom
Senior Associate
Cyber Data Privacy | Employment & Industrial Relations
E: aa@lh-ag.com

4 APRIL 2024

CYBER SECURITY BILL 2024: IS YOUR COMPANY READY?

Although Malaysia was one of the first nations within Southeast Asia to adopt a National Cyber Security Policy formulated in 2006, it does not have a single comprehensive legislation specifically for cyber security. Instead, various aspects of cyber security are covered under separate pieces of legislation such as the Computer Crimes Act 1997, Communications and Multimedia Act 1998, Personal Data Protection Act 2010, and the Penal Code.

However, last week, the Malaysian House of Representatives passed the Cyber Security Bill 2024 ("**Bill**"). The Minister of Digital, Gobind Singh Deo, during the second and third reading of the Bill, emphasised the need to strengthen the country's cyber security. This is particularly in light of the government's commitment in the application of information and communication technology to support national initiatives towards a digital economy. Hence, the Bill aims to safeguard the national critical information infrastructure ("**NCII**") by establishing a regulatory framework to govern Malaysia's cyber security landscape.

LH AG ADVOCATES AND SOLICITORS

Extra-Territorial Application

Part I of the Bill deals with preliminary matters, pertaining among others, its applicability. The Bill applies to any person, irrespective of nationality or citizenship, and has effect outside as well as within Malaysia where the NCII in respect of the offence in question is wholly or partly within Malaysia. The Bill is also binding on the Federal Government and State Governments, although they will not be liable to prosecution for any offence under the Bill.

National Cyber Security Committee ("NCSC")

Part II of the Bill deals with the establishment of the NCSC, which consists of 13 members, with the Prime Minister being the Chairman. The functions of the NCSC include, among others:

(a) to plan, formulate, and decide on policies relating to national cyber security;

(b) to decide on approaches and strategies in addressing matters relating to national cyber security;

(c) to monitor the implementation of policies and strategies relating to national cyber security;

(d) to advise and make recommendations to the Federal Government on policies and strategic measures to strengthen national cyber security; and

(e) to give directions to the Chief Executive and NCII sector leads on matters relating to national cyber security.

LH AG ADVOCATES AND SOLICITORS

Chief Executive of the National Cyber Security Agency ("Chief Executive")

Part III of the Bill provides for the duties and powers of the Chief Executive, who is also the secretary to the NCSC. The duties include, among others:

(a) to advise and make recommendations to the NCSC on policies, strategies, and strategic measures relating to national cyber security;

(b) to implement the policies, strategies, and strategic measures made, and directions given by the NCSC or the Federal Government on matters relating to national cyber security;

(c) to coordinate and monitor the implementation of policies, strategies, and strategic measures on national cyber security by the NCII sector leads, NCII entities, Government Entities, or any other person;

(d) to collect and coordinate the data, information, or intelligence relating to national cyber security received from the NCII sector leads, NCII entities, Government Entities, or any other person, and to evaluate or correlate such data, information, or intelligence;

(e) to disseminate the information and intelligence referred to in paragraph (d) to the NCII sector leads or NCII entities if the Chief Executive deems it essential to do so in the interest of national cyber security; or

(f) to issue directives to the NCII sector leads, NCII entities, Government Entities, or any

person on matters relating to national cyber security.

The Chief Executive also has a duty to establish and maintain the National Cyber Coordination and Command Centre system, a national cyber security system, for the purpose of dealing with cyber security threats and cyber security incidents.

National Critical Information Infrastructure

Part IV of the Bill deals with the NCII sector leads and entities. NCII is defined under the Bill as "*a computer or computer system which the disruption to or destruction of the computer or computer system 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 State Government to carry out its functions effectively*". The NCII sectors listed under the Bill include:

(a) Government;
(b) Banking and finance;
(c) Transportation;
(d) Defence and national security;
(e) Information, communication, and digital;
(f) Healthcare services;
(g) Water, sewerage, and waste management;
(h) Energy;
(i) Agriculture and plantation;
(j) Trade, industry, and economy; and
(k) Science, technology, and innovation.

The Bill provides for the appointment of either a Government Entity or person as the NCII sector lead ("**NCII Sector Lead**") for each of the above sectors by the Minister responsible for cyber security ("**Minister**"), upon the recommendation of the Chief

LH AG ADVOCATES AND SOLICITORS

Executive. The NCII Sector Lead shall then have the following responsibilities in respect of the NCII sector for which it is appointed:

(a) to designate any Government Entity or person which owns or operates NCII as an NCII entity ("**NCII Entity**");

(b) to prepare a code of practice containing measures, standards, and processes to ensure the cyber security of the NCII owned or operated by the NCII Entity;

(c) to implement the decisions of the NCSC and directives under the Bill;

(d) to monitor and ensure that actions required of and duties imposed on the NCII entities are accordingly carried out;

(e) to prepare and maintain guidelines on best practices in relation to cyber security management; and

(f) to prepare and submit to the Chief Executive a situational report either on its own initiative or as required by the Chief Executive where a cyber security threat or cyber security incident has affected a national critical information infrastructure within its national critical information infrastructure sector.

The Bill further provides for the following duties of an NCII Entity:

(a) To provide information to the NCII Sector Lead in respect of the NCII owned or operated by the NCII Entity as requested by the NCII Sector Lead, or where the NCII

Entity procures or has come into possession or control of any additional computer or computer system which in its opinion, is a national critical information infrastructure;

(b) To implement codes of practice;

(c) To conduct cyber security risk assessments in respect of the NCII owned or operated by the NCII Entity;

(d) To cause to be carried out an audit by an auditor approved by the Chief Executive;

(e) To notify the Chief Executive and its NCII Sector Lead on any cyber security incident which has or might have occurred in respect of the NCII owned or operated by the NCII Entity; and

(f) To comply with the directions of the Chief Executive for the purpose of cyber security exercises.

Cyber Security Service Provider

Part VI of the Bill provides for the requirement of a license in relation to any person providing or advertising as a cyber security service provider, as prescribed by the Minister. However, there has yet to be a licensing regime prescribed by the Minister.

Cyber Security Incident

Part VII of the Bill, which deals with cyber security incidents, provides for the investigation of a cyber security incident and the power of the Chief Executive to issue a directive on the measures necessary to respond to or recover from the cyber

security incident, and to prevent such cyber security incident from occurring in the future.

A cyber security incident is defined under the Bill as "*an act or activity carried out on or through a computer or computer system, without lawful authority, that jeopardises or adversely affects the cyber security of that computer or computer system or another computer or computer system*". Upon receipt of a cyber security incident notification from an NCII Entity, or if it comes to the knowledge of the Chief Executive that a cyber security incident has or might have occurred in respect of an NCII, the Chief Executive shall instruct an authorised officer to investigate into the matter.

Upon completion of the investigation, the authorised officer shall notify the Chief Executive of his findings on whether a cyber security incident has occurred or not. The Chief Executive shall then notify the NCII Entity that owns or operates the NCII. Subsequently, the Chief Executive may issue a directive to the NCII Entity on the measures necessary to respond to or recover from the cyber security incident, and to prevent such cyber security incident from occurring in the future.

The NCII Entity shall accordingly comply with the Chief Executive's directive, failing which the NCII Entity commits an offence and shall, upon conviction, be liable to a fine not exceeding RM200,000.00 or to imprisonment for a term not exceeding three years or to both.

Conclusion

The Bill, which represents a significant step towards securing Malaysia's digital era is timely, especially in view of the recent spike in cyberattacks. This signifies a paradigm shift in the national cyber security management mechanism. Therefore, it is critical that stakeholders operating in the 11 NCII

sectors specified in the Bill make the necessary preparations to comply with the numerous cyber-security related responsibilities and obligations to avoid the significant penalties for non-compliance.

If you have any queries, please contact CDP Lawyer, **Arissa Ahrom** (aa@lh-ag.com).

Head Office
Level 6, Menara 1 Dutamas
Solaris Dutamas
No. 1, Jalan Dutamas 1
50480 Kuala Lumpur
Malaysia
Tel: +603 6208 5888
Fax: +603 6201 0122

Johor Office
Suite 21.01
21st Floor, Public Bank Tower
No.19, Jalan Wong Ah Fook
80000 Johor Bahru, Johor
Tel: +607 278 3833
Fax: +607 278 2833

Penang Office
51-12-E, Menara BHL Bank,
Jalan Sultan Ahmad Shah,
10050
Penang
Tel: +604 299 9668
Fax: +604 299 9628

Email
enquiry@lh-ag.com

Website
www.lh-ag.com

Published by Cyber Data Privacy Practice