LH AG ADVOCATES AND SOLICITORS

Compliance with the New Cybersecurity Act 2024

CYBERSECURITY SERIES
OCTOBER 2024

LHAG | TECH

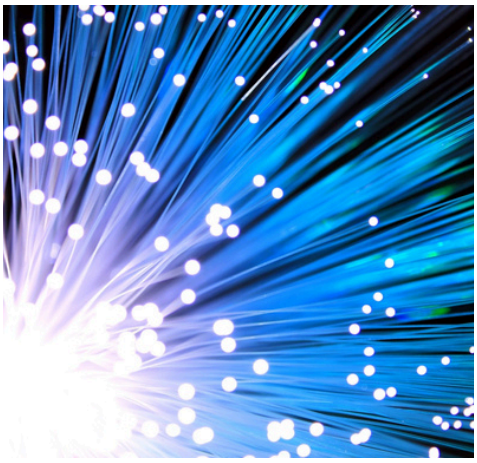
Legal updates and insights on the latest developments in the Technology, Media and Telecommunications (TMT) space.

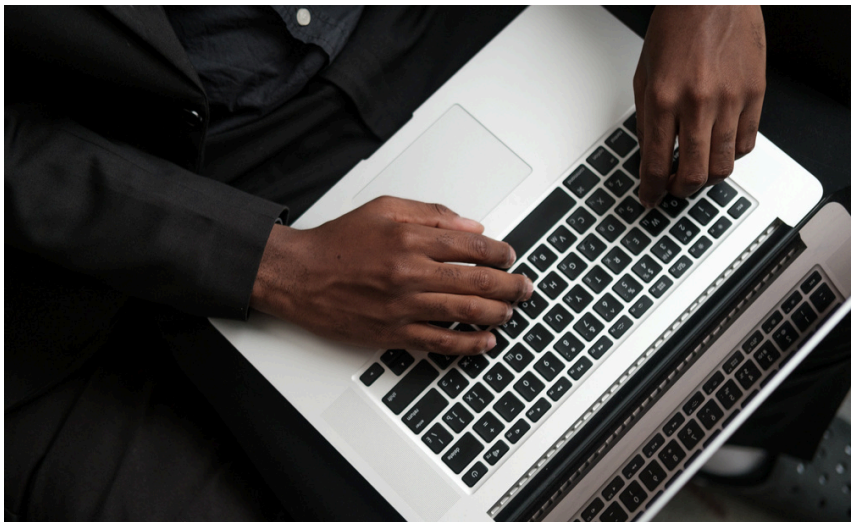
Does Your Organisation or Business Need to Comply with the New Cybersecurity Act 2024?

As we navigate an increasingly digital world and face evolving cyber threats, keeping a close eye on the impact of the Cyber Security Act 2024 ("**the Act**") and future regulatory changes is crucial. In this Cybersecurity series, we aim to provide insightful analysis on the latest developments in Malaysia's cybersecurity framework that is relevant to both public and private sectors (including private businesses) in Malaysia.

This article provides an overview of the Act and outlines who is affected by the Act. In the upcoming articles, we will further explore topics including, but not limited to:

- Compliance of the Act: A detailed look at the duties and responsibilities of the various roles defined under the Act.
- Cyber Threats and Incidents: The prevention and response to cybersecurity incidents and threats.
- Licensing of Cybersecurity Providers: Who requires a license and how to obtain it.





A New Era of Cybersecurity in Malaysia: Introduction of the Cyber Security Act 2024

Before the enactment of the Act, there was no unified legislation governing cybersecurity and related crimes. While existing laws like the Personal Data Protection Act 2010 and Communications and Multimedia Act 1998 were in place, they only regulated specific aspects of data protection and cyberspace. This piecemeal approach left significant gaps in the overall regulatory framework.

With the introduction of the Act, along with its four accompanying regulations, it is envisaged that a robust regulatory framework will be established to safeguard Malaysia's cybersecurity infrastructure. These regulations are:

1. Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024
2. Cyber Security (Licensing of Cyber Security Service Providers) Regulations 2024
3. Cyber Security (Compounding of Offences) Regulations 2024
4. Cyber Security (Notification of Cyber Security Incident) Regulations 2024

For the purpose of safeguarding Malaysia's cybersecurity infrastructure, the Act and the regulations contain provisions relating to, amongst others, the duties and powers of the Chief Executive and the National Cyber Security Agency ("**NACSA**"), the specific duties and responsibilities for national critical information infrastructure ("**NCII**") leads, the specific requirements for NCII entities to comply with to protect against cyber security threats and in Malaysia, and the mandatory requirement for any person providing or advertising as a provider of cyber security service to obtain a license.

The Act seeks to align with the borderless nature of technology where its jurisdiction covers even offences committed outside Malaysia, regardless of the offender's nationality or citizenship. However, it should be noted that the Act would only apply if the offence involved a NCII (whether located wholly or partially in Malaysia).

Additionally, the Act binds both the Federal and State Governments, which is a notable distinction from the Personal Data Protection Act 2010.

Who is affected by the Act?

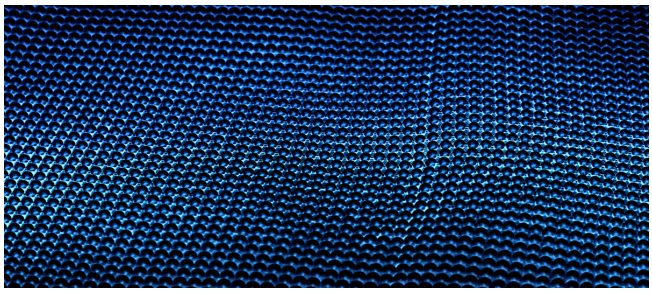
1. NCII Sectors

The Act places significant emphasis on the concept of NCII, which is defined 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 of the State Governments to carry out its functions effectively". The NCII sectors are listed in the Schedule of the Act. The Schedule of the Act clearly listed down the NCII sectors as follows:

Government	Energy
Banking And Finance	Agriculture And Plantation
Transportation	Trade, Industry and Economy
Defence And National Security	Science, Technology and Innovation
Information, Communication and Digital	Agriculture And Plantation
Healthcare Services	Water Sewerage And Waste Management

2. NCII Leads

For each sector, the Minister will appoint an NCII Sector Lead, which may be a government entity, or a designated person recommended by Chief Executive of the NACSA to carry out various important functions. This includes preparing a code of practice that details the measures, standards and processes essential necessary to safeguard the cybersecurity of the NCII within its sector.



3. NCII Entities

An NCII entity is defined as "any Government Entity or person within the identified NCII Sectors, designated as such either by an NCII Sector Lead or the Chief Executive of the NACSA. This designation occurs when the NCII Sector Lead or Chief Executive is satisfied that the Government Entity or person in question owns or operates an NCII". Private and public entities operating within an NCII Sector should note that they may be designated as an NCII Entity by the NCII Sector Lead or the Chief Executive of NACSA. If so, they are obliged to comply with specific duties under the Act which includes, but not limited to implementing the measures, standards and processes as specified in the Code of Practice.

The duties and responsibilities will be covered in depth in the next article.

4. Cyber Security Service Providers

If your business offers cybersecurity services, such as managed security operation centre monitoring or penetration testing, or advertises as providing these services, you must obtain a licence from the Chief Executive through electronic means and pay the required fees to comply with the Act.

In conclusion, organisations or businesses operating in the NCII sectors should stay updated on the latest developments in the cyber security regulatory landscape and be prepared to comply with the requirements of the Act. Additionally, businesses that offer licensable services should prepare to make the necessary application of the cyber security service provider license as required under the Cyber Security (Licensing of Cyber Security Service Providers) Regulations 2024.

In the next article, we will delve into the duties and responsibilities of the Chief Executive of NACSA, NCII Sector Leads, and NCII Entities. This will serve as a helpful guide for understanding and ensuring compliance with the Act.

For further assistance on any legal matters, please do not hesitate to contact any of the authors below.

The Authors

VIJAY KUMAR

Partner
Corporate Disputes | TMT
vkg@lh-ag.com

HARVEY NG

Associate
Corporate Disputes | TMT
nyx@lh-ag.com

KHEW GERJEAN

Associate
Corporate Disputes | TMT
kgj@lh-ag.com