Impact of the Cyber Security Act 2024 on the Cyber Security Industry

Foong Cheng Leong[*] *and Joanne Wong Min Min*[**]

Abstract

The Cyber Security Act 2024 ("the Act") together with four subsidiary legislation[1] came into force on August 26, 2024. The Act aims to help the government ensure the implementation and efficiency of national critical information infrastructure functions in addressing cyber security incidents. While the Act offers numerous benefits, such as promoting compliance, fostering collaboration, tailoring security measures to specific sectors, ensuring consistency, and increasing the need for cyber security professionals and services, it also presents challenges, particularly for smaller entities facing financial constraints due to the costs of compliance. The licensing requirement for cyber security service providers, though aimed at ensuring high standards, may be drafted too broadly and may stifle innovation. By examining the Act's objectives, benefits, and potential challenges, this article aims to offer an impartial assessment of its implications for Malaysia's cyber security landscape, particularly in the area of the requirements of the code of practice, audits and licensing of cyber security service providers.

Introduction

In the case of *Rose Hanida bt Long v Pendakwa Raya*,[2] Judicial Commissioner Mohamad Shariff Abu Samah held that the abuse of national critical information infrastructure ("NCII") challenges a nation's dignity and integrity. Such an attack will ultimately affect the future of the nation's industries by compromising the reputation of essential services and eroding public confidence. An attack must be looked at seriously and be condemned strongly by the community. Given its importance, it is crucial to have cyber security laws protecting the NCII of our country.

---

[*] Cheng Leong is an Advocate and Solicitor of the High Court of Malaya. He is the author of *Foong's Malaysia Cyber, Electronic Evidence and Information Technology Law* (Thomson Reuters Malaysia/Sweet & Maxwell, 2020).

[**] Joanne is a law student at Help University. She was a former intern at the firm of Foong Cheng Leong & Co

[1] The four (4) regulations are Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024, Cyber Security (Notification of Cyber Security Incident) Regulations 2024, Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024 and Cyber Security (Compounding of Offences) Regulations 2024.

[2] [2017] MLJU 1212.

On April 3, 2024, the Cyber Security Bill 2024 was passed by Parliament.

This new law aims to enhance national cyber security by providing for the establishment of the National Cyber Security Committee ("NCSC"), the duties and powers of the Chief Executive of the National Cyber Security Agency, the functions and duties of the NCII sector leads and NCII entities, and the management of cyber security threats and incidents to NCIIs, to regulate cyber security service providers through licensing and to provide for related matters.[3]

Cyber security legislation is not a new concept. Various countries have enacted laws to address this critical issue: Singapore enacted the Cybersecurity Act 2018; Thailand enacted the Cyber Security Act 2019; Vietnam enacted the Law on Cyber Security in 2018; the EU enacted the Cybersecurity Act (EU 881/2019); Australia enacted the Security of Critical Infrastructure Act in 2018; and Ghana enacted the Cybersecurity Act 2020.

Though bearing similarities to other foreign cyber security legislation, the Act brings forth unique positions such as the Chief Executive and the NCII sector lead. These roles are designed to provide a more industry-tailored approach to cyber security governance within Malaysia.

Amid the rising cyber breaches in Malaysia, the Act marks a crucial step towards a secure digital future. It highlights the nation's dedication to safeguarding NCII in both public and private sectors through proposed measures, standards and processes.

Brief history of cyber security laws in Malaysia

Prior to the introduction of the Act, Malaysia did not have an all-encompassing cyber security legislation to safeguard digital infrastructure and the cyber domain. Cyber security requirements existed across multiple legislation, such as the Personal Data Protection Act 2010, the Communications and Multimedia Act 1998, the Computer Crimes Act 1997 and others. Regulated entities are also subject to cyber security standards prescribed by the regulating authority. For example, the Securities Commission of Malaysia has issued the Guidelines on Management of Cyber Risk in October 2016 and the Guidelines on Technology Risk Management in August 2023.

The National Cyber Security Agency ("NACSA") was established as the lead agency on national cyber security and is responsible for all aspects of cyber security based on policies and strategic measures formulated by the National Security Council[4] with the objectives of securing and strengthening Malaysia's resilience in facing the threats of cyberattacks by coordinating

[3] Cyber Security Act 2024, Long title.

[4] The National Security Council is a federal agency under the Prime Minister's Department.

and consolidating the nation's best experts and resources in the field of cyber security. One of NACSA's aims is to protect the NCII.

The establishment and roles of NACSA are further strengthened by the National Security Council's Directive No. 26 on National Cyber Security Management. The National Security Council's Directive No. 26 is an executive directive that defines the overall governance of Malaysia's cyber security ecosystem. The roles and responsibilities of every stakeholder are delineated to ensure understanding and seamless implementation of national cyber security initiatives and strategy. The objectives of this directive are to: (a) establish a comprehensive national cyber security management structure and outline the roles and responsibilities of agencies in the national cyber security ecosystem; (b) achieve a uniform and proactive approach so that national cyber security management can be implemented effectively; and (c) outline the duties and responsibilities of the National Security Council, the Prime Minister's Department as the focal point for Malaysia's cyber security matters through NACSA.[5]

However, the National Security Council Act 2016 does not grant NACSA any regulatory or enforcement authority. It provides the necessary powers for national security enforcement to the National Security Council but does not give NACSA the necessary regulatory and enforcement powers for cyber security.

There is also no specific legislation addressing national cyber security issues and threats, particularly responses needed to neutralise cyber security threats and incidents, and the maintenance of cyber hygiene through the imposition of cyber security audits and risk assessments.

Despite the existence of legislation related to cyber crime and cyber security in Malaysia, it is important to enact new laws considering the emergence of new cyber threats. It is provided that on the date of the coming into operation of the Act, any measures, standards and processes which have been implemented to ensure the cyber security of a NCII and imposed on any government entity or person under the Directive of the National Security Council No. 26 shall, as long as they are consistent with the provisions of the Act, continue to remain in force until they are revoked under the National Security Council Act 2017.[6]

Applicability of the Act

The Act has extra-territorial effect and shall apply in relation to any person, regardless of nationality or citizenship and shall have effect outside as well as within Malaysia.[7]

---

[5] Malaysia Cyber Security Strategy, 2020–2024, p 7.
[6] Cyber Security Act 2024, s 64.
[7] *Ibid*, s 3.

In practice, it may, however, be difficult to apprehend transnational cybercriminals, especially if the criminals are often based in jurisdictions with weaker laws and enforcement. The increase in extraterritorial reach may have a limited impact on preventing or deterring these criminals.

While the federal government and state governments are also subject to the Act, no prosecution action can be taken against them for any failure to comply with the provisions of this law within this legislation.[8] It is provided that in terms of government administration, the government will take all necessary steps to ensure that the provisions of this legislation are fully complied with by agencies under the federal government and also agencies under the state governments.[9]

National critical information infrastructure

The Act introduces the concept of NCII. It is defined as "*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*."[10]

For instance, computer or computer systems utilised in sectors such as government; banking and finance; transportation; defence and national security; information; communication and digital; healthcare services; water, sewerage and waste management; energy, agriculture and plantation; trade, industry and economy, and science technology and innovation.[11]

National Cyber Security Committee

The Act establishes the NCSC, consisting of the Prime Minister, the ministers responsible for certain government bodies and agencies, the Chief Secretary to the Government, the Chief of Defence Force, the Inspector General of Police, the Director General of National Security and two other persons who shall be appointed by the Committee from among persons of standing and experience in cyber security.

The functions of the NCSC include:[12]

(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;

---

8 *Ibid*, s 2(2).
9 *Hansard*, Second Reading in the House of Representatives on March 27, 2024, pp 39-40.
10 Cyber Security Act 2024, s 4.
11 *Ibid*, First Schedule.
12 *Ibid*, s 6(1).

(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;

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

(f) to oversee the effective implementation of the Act; and

(g) to do such other things arising out of or consequential to the functions of the Committee under the Act consistent with the purposes of the Act.

The NCSC shall have all such powers as may be necessary, or in connection with, or reasonably incidental to, the performance of its functions under the Act.[13]

The Chief Executive

The Act creates a Chief Executive of the National Cyber Security Agency ("Chief Executive") and he is the secretary of the NCSC.

The Chief Executive is empowered under the Act to, among others, advise and make recommendations to the NCSC,[14] implement policies relating to cyber security,[15] appoint a cyber security expert,[16] conduct a cyber security exercise for the purpose of assessing the readiness of any NCII entity in responding to any cyber security threat or cyber security incident,[17] establish the National Cyber Coordination and Command Centre system for the purpose of dealing with cyber security threats and cyber security incidents[18] and issue directives as necessary for the purpose of ensuring compliance with the Act.[19]

The Chief Executive is given very wide powers under s 14. Under s 14(1), the Chief Executive has the power to direct for information. He may require any person, public body, or corporation to provide information, particulars, documents, or evidence within a specified period of time and in a specific manner if he has reasonable grounds to believe that they possess such information relevant to his duties and powers. Failure of any person to

[13] *Ibid*, s 6(2).
[14] *Ibid*, s 10.
[15] *Ibid*.
[16] *Ibid*, s 12.
[17] *Ibid*, s 24.
[18] *Ibid*, s 11.
[19] *Ibid*, s 10.

comply with the request is liable to a fine not exceeding RM200,000 and/or to imprisonment for a term not exceeding three years.[20]

The power of the Chief Executive is broad under this section because the Chief Executive can issue written notices to "any person" for the production of information, documents, or electronic media on a schedule "as specified" or otherwise determined by the Chief Executive. Though the duties and powers of the Chief Executive are set out in s 10, s 14 is still broadly worded and this may lead to abuse or excessive or improper exercise.

The direction for information is not subject to any external review process and is entirely at the discretion of the Chief Executive in substance and procedure. It is also noted that s 14(1) uses the term "any person". This deliberate choice of term seems to suggest that the Chief Executive may request such information from any person, regardless of whether they own or operate any NCII.

In any event, it is submitted that the Chief Executive , like any other entities, should go through a court process to obtain information or documents. Nevertheless, an aggrieved person may challenge the direction of the Chief Executive by way of judicial review.

Under s 14(2), if the recipient of such a request does not possess the document, they shall state, to the best of their knowledge and belief, where the document may be found, and identify, to the best of their knowledge and belief, the last person who had custody of the document, as well as stating, to the best of their knowledge and belief, where that last-mentioned person may be found.

Under s 14(3), the recipient of such a request, shall ensure that the information, particulars or, documents, or copies of the document given or produced are true, accurate and complete, and such person shall provide an express representation to that effect, including a declaration that he is not aware of any other information, particulars or document which would make the information, particulars or document given or produced untrue or misleading.

Failure of any person to comply with s 14(2) and/or 14(3) will be liable to a fine not exceeding RM200,000 or to imprisonment for a term not exceeding three years or both.

NCII sectors

The Act sets out the following list of sectors regarded as NCII sectors (each a "NCII sector") that are crucial to Malaysia's cyber security:

[20] *Ibid*, s 14(6).

(a) the 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.[21]

NCII sector lead and NCII entity

The Act introduces two types of persons, namely, the NCII sector lead and the NCII entity.

The Act defines NCII sector lead as "*any Government Entity or person appointed as a national critical infrastructure sector lead for each of the NCII Sector*".[22] The minister responsible for cyber security ("minister") may, upon the recommendation of the Chief Executive, appoint any government entity or person as the NCII sector lead for each of the NCII sectors. Each NCII sector may have one or more NCII sector lead(s).[23]

NCII sector leads will be tasked with, among others, to:[24]

(a) designate any government entity or person as an entity which owns or operates NCII for their appointed sector;

(b) prepare a code of practice containing measures, standards and processes it to ensure the cyber security of an NCII within their appointed NCII sector ("Code of Practice");

(c) implement the decisions of the NCSC and directives made under the Act; and

---

21 *Ibid*, First Schedule.
22 *Ibid*, s 4.
23 *Ibid*, s 15.
24 *Ibid*, s 16.

(d) monitor and ensure that NCII entities carry out obligatory duties imposed upon them.

NCII entity is defined as "*any Government Entity or person designated as an NCII Entity by a NCII Sector Lead, designated in such a manner as may be determined by the Chief Executive, if the NCII Sector Lead is satisfied that they own or operate an NCII*".[25] The Chief Executive may also designate a NCII sector lead as an NCII entity if satisfied that the NCII sector lead owns or operates an NCII.[26]

Government entity means any ministry, department, office, agency, authority, commission, committee, board, council or other body, of the federal government, or of any of the state governments, established under any written law or otherwise; and any local authority.[27] Notably, a government entity can only be designated as an NCII entity by an NCII sector lead which is itself a government entity.[28]

The NCII entity may lose its designation if the NCII sector lead, or the Chief Executive (in the case where the NCII sector lead itself is an NCII entity), is satisfied that the NCII entity no longer owns or operates any NCII.[29]

The duties of the NCII entity include, among others, to:

(a) *Code of Practice*: Implement the measures, standards and processes as specified in the Code of Practice.[30]

(b) *Audit*: Cause to be carried out an audit to determine the compliance of the NCII entity with the Act.[31]

(c) *Cyber risk assessments*: Conduct cyber risk assessments in accordance with the Code of Practice and directive.[32]

(d) *Cyber security incident*: Notify the Chief Executive and the relevant NCII sector lead(s) of any cyber security incident[33] which has or might have occurred in respect of the NCII owned or operated.[34]

---

[25] *Ibid*, s 17.
[26] *Ibid*, s 18.
[27] *Ibid*, s 4.
[28] *Ibid*, s 17(3).
[29] *Ibid*, s 19.
[30] *Ibid*, s 21(1).
[31] *Ibid*, s 22(1)(b).
[32] *Ibid*, s 22(1)(a).
[33] *Ibid*, s 4. Cyber security incident is defined 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".
[34] *Ibid*, s 23(1).

(e) *Provision of information*: Provide information relating to NCII owned or operated when there is a request by the NCII sector lead(s), when the NCII entity procures or comes into possession or control of any additional computer or computer system which, in its opinion, is an NCII, or when a material change is made to the design, configuration, security or operation of the NCII.[35]

The above requirements are further explained below.

Code of Practice

Section 25 requires the NCII sector lead to prepare a Code of Practice which will be implemented by the NCII entity to ensure the cyber security of the NCII. The Code of Practice shall contain measures, standards and processes to ensure the cyber security of an NCII within the NCII sector. The Code of Practice may be endorsed by the Chief Executive who will do so if the Chief Executive is satisfied that it fulfils the requirements of s 25(3).

In preparing the Code of Practice, the NCII sector lead shall consider, among others, the following matters:

(a) the functions of the relevant NCII entities;

(b) provisions relating to cyber security under any other written law applicable to the NCII sector lead;

(c) the views of the relevant NCII entities; and

(d) the views of the relevant regulatory authority, if any,

of which the NCII entity is subject to.

Failure by the NCII sector lead to prepare a Code of Practice is an offence and it will be liable to a fine not exceeding RM100,000.[36]

Pursuant to s 21(2), notwithstanding the cyber security measures in the Code of Practice, the Act allows NCII entities to implement alternative measures, standards, and processes if the NCII entity can prove to the satisfaction of the Chief Executive that they offer an equal or higher level of protection to the NCII.[37] NCII entities may also establish and implement additional internationally recognised standards or frameworks.[38] This flexibility enables organisations to adapt cyber security strategies according to their circumstances, ensuring that the prescribed measures are both effective and feasible for implementation.

---

35 *Ibid*, s 20.
36 *Ibid*, s 25(6).
37 *Ibid*, s 21(2).
38 *Ibid*, s 21(3).

Additionally, where an NCII entity implements measures, standards and processes to ensure the cyber security of its NCII as required under any other written law, the NCII entity shall be deemed to have complied with the Code of Practice, provided that such measures, standards and processes are not in contravention of it.[39]

Advantages of a Code of Practice

A Code of Practice sets a legal framework for cyber security standards. By outlining specific requirements, guidelines, best practices, and minimum standards, a Code of Practice provides clarity and consistency in cyber security expectations across various sectors and industries. This is essential for ensuring that organisations understand their obligations and responsibilities, thereby promoting a culture of compliance and accountability. By imposing penalties on entities that fail to meet the prescribed standards,[40] it is clear that cyber security is not optional but a legal obligation that must be taken seriously.

Furthermore, a Code of Practice can establish a partnership between the industry and government to regulate the cyber security ecosystem. This partnership uses a co-regulatory approach where NCII sector leads can determine the regulations for their sector's cyber security. It can also foster collaboration, accountability, and deterrence between the NCII sector leads, NCII entities, government and cyber security professionals.

Sections 25(2)(c) and (d) provide that, when preparing the Code of Practice, the NCII sector lead is required to consider the views of the relevant NCII entities and the views of the relevant regulatory authority, if any, to which the NCII entity is subject.[41] Thus, this ensures adequate industry consultation and collaboration and is crucial for both the development and implementation of a Code of Practice.

Besides, s 25(2)(a) provides that the NCII sector lead shall consider the functions of the relevant NCII entities while preparing a Code of Practice. Therefore, a Code of Practice could tailor to the nuances and unique risks of the industry, ensuring that cyber security measures are not only relevant but also effective in addressing specific issues or concerns within each different industry or sector. For example, the cyber security needs of the financial sector, with its emphasis on data privacy and transaction security, may differ significantly from those of the healthcare sector, which prioritises the protection of sensitive patient information. By taking into account the unique functions and risks associated with each industry, a Code of Practice can

---

[39] *Ibid*, s 21(4).

[40] *Ibid*, s 21(5) provides that failure of the NCII entity to implement the Code of Practice is liable to a fine not exceeding RM500,000 and/or imprisonment for a term not exceeding 10 years.

[41] *Ibid*, s 25(2).

provide targeted guidance on implementing appropriate safeguards and controls.

A Code of Practice also serves as a mechanism for ensuring consistency in the implementation of cyber security measures across NCII entities. Section 26 outlines that when an NCII sector lead directs any NCII entity to implement measures, standards and processes to ensure the cyber security of the NCII, owned or operated by the NCII entity under any other written law, the NCII sector lead shall ensure that the directions given are consistent with the Code of Practice. This ensures uniformity in cyber security practices across different NCII sectors and NCII entities. It also provides a clear framework for NCII sector leads to follow when issuing directives, ensuring that their decisions are guided by established practices and industry standards. This helps to mitigate the risk of arbitrary or inconsistent enforcement of cyber security requirements, fostering trust and confidence in the regulatory regime.

A Code of Practice can also serve as a valuable complement to address any inadequacies or ambiguities present in the Act. By providing additional guidance and clarification on specific aspects of cyber security implementation and compliance such as technical requirements and procedural protocols that may not be explicitly addressed in the legislation, the Code of Practice can help fill any gaps or uncertainties within the legislation. This ensures that organisations have a comprehensive framework to follow when implementing cyber security measures, enhancing the effectiveness and enforceability of cyber security laws.

Considering its benefits, it is anticipated that these advancements could also be extended to non-critical information infrastructure.

Disadvantages of Code of Practice

Some NCII entities may face challenges while adhering to the measures within the Code of Practice due to several reasons. For instance, financial constraints could pose a significant hurdle for some NCII entities as implementing these measures may demand higher overhead costs and substantial investments in advanced technological infrastructure, specialised software, or hardware upgrades in key areas such as security monitoring and compliance.

Furthermore, they may even need to adopt cutting-edge technology solutions, automation, and AI solutions to enhance capabilities and keep pace with evolving threats. This raises concerns about whether the burden of compliance will be shifted onto consumers and if it might impact economic competitiveness and foreign investment. Nevertheless, it is clear that while compliance expenses may rise, the extensive measures align with the prevailing global trend and a robust cyber security environment could actually be appealing to foreign investors.

Audit

Pursuant to s 22, an NCII entity is required to carry out an audit by an auditor approved by the Chief Executive and submit the same to the Chief Executive to determine the compliance of the NCII entity with the Act.[42] Under reg 3(b) of the Cyber Security (Period for Cyber Security Risk Assessment and Audit) Regulations 2024, a NCII entity shall carry out an audit at least once every two years or at such higher frequency as may be directed by the Chief Executive in any particular case.

The audit report will need to be submitted to the Chief Executive within 30 days after the completion of the report.[43] Insufficient audit reports submitted to the Chief Executive necessitate rectification under the Chief Executive's directives.[44] The Chief Executive may cause an audit to be carried out if a material change was made to the NCII regardless of whether the audit has been carried out before.[45] The Chief Executive may also direct an NCII entity to carry out an additional audit.[46]

Failure of the NCII entity to submit the audit report is an offence and it will be liable to a fine not exceeding RM200,000 and/or imprisonment for a term not exceeding three years.[47]

Advantages of audit

Regular audits are crucial components of a comprehensive security strategy. The implementation of regular audits and compliance checks could ensure that the cyber security measures are up to the mark and that the organisation is adhering to the established regulations, thereby enhancing cyber security measures within organisations. This can help protect the organisation from legal liability that will result in financial consequences and reputational risks.

The Act does not impose this requirement on the entire business community. Instead, it is designed to regulate the NCII, which is vital at a national level, as their disruption or compromise could significantly impact Malaysia's survival, security, safety, or other national interests. This focused approach targets a specific set of systems and entities, acknowledging that while compliance costs are inevitable, the goal is to avoid undue regulatory burden. Hence, organisations operating with NCII should rightfully bear the corresponding costs as their operations are crucial to national security and interests.

---

42 *Ibid*, s 22(1)(b).
43 *Ibid*, s 22(2).
44 *Ibid*, s 22(4).
45 *Ibid*, s 22(5).
46 *Ibid*, s 22(6).
47 *Ibid*, s 22(7).

Besides, conducting comprehensive audits allows organisations to proactively assess the adequacy of their current security strategies and identify potential vulnerabilities. An audit can also help organisations to better understand and manage their cyber security risks. This can help reduce the likelihood of a data breach or other security incidents and enhance the organisations' capacity in compliance with the Act.

Moreover, the requirement of reporting can ensure the consistency of information.[48] This uniformity not only helps in maintaining a high level of security across the sector, but also streamlines regulatory oversight. Consistent reporting fosters transparency and accountability, enabling more accurate assessments of the overall cyber security landscape and fostering trust and safety for all stakeholders.

Conducting audits can also enhance customer confidence in an organisation's ability to protect their data. This increased trust can lead to higher sales and revenue, further strengthening the organisation's reputation and customer relationships.

Disadvantages of audit

The disadvantage of this aspect is similar to the concern in the Code of Practice, which is the financial resources required to comply, as appointing an auditor with expertise can be costly, and subscription to additional insurance such as cyber insurance.

Cyber risk assessment

Pursuant to s 22(1)(a), the NCII entity shall conduct a cyber security risk assessment within the period as may be prescribed in respect of the NCII in accordance with the Code of Practice and directive. Regulation 2 of the Cyber Security (Period for Cyber Security Assessment and Audit) Regulations 2024 defines "cyber security risks" as "*the risks that a vulnerability in the cyber security of the NCII be exploited by a cyber security threat or cuber security incident*".

Under reg 3(a) of the Cyber Security (Period for Cyber Security Assessment and Audit) Regulations 2024, a NCII entity shall conduct a cyber security risk assessment at least once a year.

The cyber security risk assessment report will need to be submitted to the Chief Executive within 30 days after the completion of the report.[49] Where the Chief Executive is not satisfied with the result of the cyber security risk assessment, the Chief Executive may direct the NCII entity to take further initiatives to re-evaluate the cyber security risk to such NCII within the

[48] Presentation slides provided at the public dialogue session of the Cyber Security Bill dated November 24, 2023.

[49] Cyber Security Act 2024, s 22(2).

period as may be determined by the Chief Executive.[50] The Chief Executive may direct the NCII entity to conduct a cyber security risk assessment if a material change was made to the NCII, regardless of whether the cyber security risk assessment has been conducted before.[51] The Chief Executive may also direct an NCII entity to conduct an additional cyber security risk assessment.[52]

Failure of the NCII entity to conduct cyber security risk assessments in accordance with the Code of Practice and directive, and to carry out an audit, is an offence. It will be liable for a fine not exceeding RM200,000 and/or imprisonment for a term not exceeding three years.[53]

Cyber security incident

Pursuant to s 23, the NCII entity shall notify the Chief Executive and the relevant NCII sector lead(s) of any cyber security incident[54] which has or may have occurred in respect of the NCII owned or operated. This shall be done by an authorised person of a NCII entity immediately by electronic means when the cyber security incident comes to the knowledge of the NCII entity.[55]

Regulation 2 of the Cyber Security (Notification of Cyber Security Incident) Regulations 2024 provides for the period of notification and particulars of information. Regulation 2(2) provides that within six hours from the time the cyber security incident comes to the knowledge of the NCII entity, the authorised person shall submit the following particulars of information:

(a) particulars of the authorized person;

(b) the particulars of the NCII entity concerned, the NCII sector and the NCII sector lead to which it relates; and

(c) the information of 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 of the occurrence of the cyber security incident is known; and

(iv) the method of discovery of the cyber security incident.

---

50 *Ibid*, s 22(3).
51 *Ibid*, s 22(5).
52 *Ibid*, s 22(6).
53 *Ibid*, s 22(7)
54 *Ibid*, s 4. Cyber security incident is defined 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".
55 Cyber Security (Notification of Cyber Security Incident) Regulations 2024, reg 2(1).

Regulation 2(3) provides that within 14 days after the notification of the cyber security incident, the authorized person shall provide to the fullest extent practicable the following supplementary information:

(a) the particulars of the NCII affected by the cyber security incident;

(b) the estimated number of host 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; and

(h) the action taken.

The submission of information under sub-regulations 2(2) and 2(3) of the Cyber Security (Notification of Cyber Security Incident) Regulations 2024 shall be made through the National Cyber Coordination and Command Centre System or in the event of disruption in the National Cyber Coordination and Command Centre System, by the communication as may be determined by the Chief Executive.

Besides, the authorised person of the NCII entity shall provide, from time to time, further updates on the cyber security incident as the Chief Executive may require.[56]

Upon receipt of the incident report, the Chief Executive will instruct an authorised officer[57] to investigate the matter.[58] The purpose of the investigation is to ascertain if it in fact occurred and determine rectification and preventative measures to prevent the incident from occurring in the future.[59]

Upon completion of the investigation by the authorised officer, if the authorised officer finds that:

(a) no cyber security incident has occurred, the authorised officer shall notify the Chief Executive about such findings and the Chief

[56] *Ibid*, reg 2(4).
[57] Cyber Security Act 2024, s 4 provides that an authorised officer means any police officer of whatever rank or any public officer authorised by the minister.
[58] *Ibid*, s 35(1).
[59] *Ibid*, s 35(2).

Executive shall notify the NCII entity accordingly and dismiss the matter; or,

(b) if the authorised officer finds that a cyber security incident has occurred, the authorised officer shall notify the Chief Executive about such findings and the Chief Executive shall notify the NCII entity accordingly.

Upon being notified by the authorised officer that a cyber security incident has occurred, the Chief Executive may issue a directive to the NCII entity concerned 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.[60]

Failure of the NCII entity to comply with the directive of the Chief Executive 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 is an offence, and it will be liable to a fine not exceeding RM200,000 and/or imprisonment for a term not exceeding three years.[61]

Provision of information relating to NCII

Pursuant to s 20, the NCII entity shall provide information relating to NCII owned or operated upon a request by the NCII sector lead(s). Where the NCII entity procures or has come into possession or control of any additional computer or computer system which in the opinion of the NCII entity is a NCII, the NCII entity shall provide such information to its NCII sector lead regardless whether there is a request. If a material change is made to the design, configuration, security or operation of the NCII owned or operated by the NCII entity after the information on such NCII has been provided, the NCII entity shall notify its NCII sector lead of the material change within 30 days from the date the change was completed. The NCII sector lead shall notify the Chief Executive of any information received in relation to the additional NCII or the material change that is made to the NCII in the manner as may be determined by the Chief Executive.[62]

Failure of the NCII entity to comply with the NCII sector lead's request for the provision of information in relation to the NCII is an offence and it is liable to a fine not exceeding RM100,000 and/or two years or both.[63]

Licensing of cyber security service providers

Importantly, the Act introduces a licensing framework for cyber security service providers. A cyber security service provider is defined as "*a person*

[60] *Ibid*, s 35.
[61] *Ibid*, s 35(5).
[62] *Ibid*, s 20.
[63] *Ibid*.

who provides a cyber security service, where cyber security service is defined as *any cyber security service that may be prescribed by the Minister for which a licence shall be obtained*".[64]

As per s 27 of the Act, person who:

(a) provides any cyber security service; or

(b) advertises, or in any way holds himself out as a provider of a cyber security service, shall hold a licence to provide a cyber security service.

The application for the licence or for the renewal of licence shall be made to the Chief Executive through electronic means and shall be accompanied by payment of a prescribed fee.[65] An application may be withdrawn at any time before the application is approved or refused by the Chief Executive.[66] The fee shall be payable for every application submitted and shall not be refundable.[67] A person who, in connection with any application made under these regulations, makes a statement that is false or misleading knowing it to be false or misleading or willfully omits to state any matter or thing without which the application is misleading commits an offence, and shall, on conviction, be liable to a fine not exceeding RM 50,000 or to imprisonment for a term not exceeding two years or to both.[68]

The Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024 provides for two (2) types of cyber security services that require licensing and they are managed security operation centre monitoring service[69] and penetration testing service.[70] Regulation 2(2) of the Cyber

---

64 *Ibid*, s 4.

65 Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024, regs 6(1), 7(1).

66 *Ibid*, regs 6(2), 7(2).

67 *Ibid*, regs 6(3), 7(3).

68 Under reg 8 of the Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024.

69 Regulation 4 of the Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024 defines managed security operation centre monitoring service as 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.

70 Regulation 5 of the Cyber Security (Licensing of Cyber Security Service Provider) Regulations 2024 defines penetration testing service as a service for assessing, testing or evaluating the level of cyber security of a computer or computer system, by searching for vulnerabilities ("vulnerability" is interpreted as any vulnerability on a computer or computer system that can be exploited by one or more cyber security threats in the same regulations) 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 (Licensing of Cyber Security Service Provider) Regulations 2024 provides that these regulations shall not apply if:

(a) the cyber security service is provided by a Government Entity;

(b) the cyber security service is provided by a person, other than a company, to its related company; or

(c) the computer or computer system in respect of which the cyber secirity service is provided is located outside Malaysia.

Similarly, the Singapore Cybersecurity Act 2018 also sets out the same types of service providers, that is, penetration testing[71] and managed security operations centre monitoring.[72]

These two services are given precedence due to the sensitive data they handle from clients. They are also widely used in the Singapore market, making them influential in shaping overall security measures. The decision to limit the licensing framework to these two services also considers industry concerns that broader licensing requirements could hinder the growth of a vibrant cyber security ecosystem in Singapore and impede assistance from global cyber security providers on short notice.

---

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 organization'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) utilizing social engineering to assess the level of vulnerability of an organization to cyber security threats.

71 Penetration testing service is defined in the Second Schedule to the Singapore Cybersecurity Act 2018 as a service for assessing, testing or evaluating the level of cyber security of a computer or computer system by searching for vulnerabilities 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 incidents through simulation of attempts to penetrate the cyber security defences of the computer or computer system; (c) identifying and quantifying the cyber security vulnerabilities of a computer or computer system, indicating vulnerabilities and providing appropriate mitigation procedures required to eliminate vulnerabilities or to reduce vulnerabilities to an acceptable level of risk; (d) utilising social engineering to assess the level of vulnerability of an organisation to cyber security threats.

72 Managed security operations centre (SOC) is defined in the Second Schedule to the Singapore Cybersecurity Act 2018 as a service for the monitoring of the level of cyber security of a computer or computer system of another person. This is done by acquiring, identifying and scanning information that is stored in, processed by, or transmitted through the computer or computer system to identify cyber security threats.

Any person or entity that provides cyber security services or holds themselves out as a provider of cyber security service without a licence shall be liable to a fine not exceeding RM500,000 and/or imprisonment for a term not exceeding 10 years.[73]

Foreign companies who provide cyber security services in Malaysia are also required to register as a cyber security service provider.[74]

According to s 28, an applicant must not have any convictions for offences involving fraud, dishonesty, or moral turpitude. Additionally, the Chief Executive shall establish other prerequisite requirements for applying for a licence.[75] Under s 29, when the Chief Executive receives the application for licence, the Chief Executive may approve the application and issue to the applicant a licence upon payment of the prescribed fee in such form as may be determined by the Chief Executive. If the Chief Executive refuses a licence application, he must provide the reasons for refusal.[76] The Chief Executive may issue a licence that is subject to such conditions as the Chief Executive thinks fit to impose and the Chief Executive may at any time vary or revoke the conditions imposed on a licence.[77]

Licensees also have a duty to keep and maintain records. They must record particulars such as the name of the licence holder or any person acting on his behalf, details of the services provided and any other particulars the Chief Executive requires.[78] The records shall be kept and maintained in the manner as determined by the Chief Executive; retained for a period of not less than six years from the date the cyber security service was provided; and produced to the Chief Executive at any time as directed by the Chief Executive.[79]

Advantages of licensing of cyber security service providers

This initiative seeks to prioritise the protection of user data and enforce accountability within the industry.

The licensing requirement is deemed essential due to the rising cyber security risks and the extensive access that cyber security providers have to clients' computers and networks, which may expose them to system vulnerabilities. This underscores the government's serious approach to regulating cyber security services and emphasises the significance of complying with licensing regulations.

---

73 Cyber Security Act 2024, s 27.
74 *Hansard*, Second Reading at Senate, p 138.
75 Cyber Security Act 2024, s 28(a)–(b).
76 *Ibid*, s 29(3).
77 *Ibid*, s 31.
78 *Ibid*, s 32(1).
79 *Ibid*, s 32(2).

The licensing requirement enables the Chief Executive to oversee and regulate the operations of the licensed entities and enables enhancement of the standard of quality of service providers. It ensures that the cyber security service providers meet specific qualifications and adhere to established guidelines, thereby improving the overall quality, safety and security of services provided, leading to a better protection of user data against cyber threats and breaches. This promotes the development of the cyber security service provider in Malaysia and raises professional standards, skill levels and expertise in the field of cyber security. This can help Malaysia promote confidence and attract international partners, customers and investors, positioning itself as a leading digital hub in ASEAN, and contributing to economic growth.

Additionally, licensing requirements can address information asymmetry, that is, where one party has more or superior information compared to another. The framework may set standardised criteria for the qualifications, work function and capabilities of cyber security service providers. This means that all licensed providers meet a minimum standard of expertise and reliability. It promotes consistency and cohesiveness, benefitting not only service providers by providing clear guidelines but also ensuring uniformity in service delivery for customers. It would also help trade and businesses make an informed decision when selecting a cyber security service provider.

In fact, cyber security has been identified as a tech enabler under the Program Mangkin Malaysia Digital (Pemangkin).[80] In 2023, the Malaysia Digital Economy Corporation (MDEC) allocated RM238 million for the 2023–2025 period to support new initiatives under Pemangkin, including RM45 million for tech enablers.[81] In light of these initiatives, licensed cyber security service providers may apply for the Malaysia Digital Status which offers tax incentives, foreign knowledge worker quota and passes, and community benefits such as business matching and partnerships.[82]

The introduction of licensing requirements is also likely to increase the demand for cyber security professionals and skills. Organisations may be compelled to invest in talent acquisition and development initiatives to comply with regulatory standards and obtain licences. This ensures a competitive landscape where cyber security professionals are valued and incentivised to continuously enhance their expertise. Ultimately, the

[80] MDEC, available at https://mdec.my/malaysiadigital (accessed July 15, 2024).

[81] Bernama, "Govt Identifies RM1 Billion Potential Investments in Nine Sectors Under Pemangkin", *New Straits Times* (Malaysia, April 17, 2023), available at https://www.nst.com.my/news/nation/2023/04/900499/govt-identifies-rm1-billion-potential-investments-nine-sectors-under (accessed July 15, 2024).

[82] Hui Lynn Tan, "Malaysia: Keeping up with Growing Cyber Threats and Intrusions – Malaysia's Cyber Security Bill 2024", *DFDL* (April 1, 2024), available at https://www.dfdl.com/insights/legal-and-tax-updates/malaysia-keeping-up-with-growing-cyber-threats-and-intrusions-malaysias-cyber-security-bill-2024/ (accessed July 15, 2024).

licensing framework serves as a catalyst for nurturing talent and elevating industry standards. The enhanced capacity will enable organisations to handle more sophisticated attacks and enhance their abilities to prevent, detect and respond to them promptly.

Disadvantages of licensing of cyber security service providers

The Chief Executive may register certifying agencies including agencies outside Malaysia to certify compliance codes or any standards under the Act.[83] It could be seen that the scope of this provision is broad and the minister is given the blanket authority to prescribe any cyber security service.

In addition to the vague definition of "cyber security service", another notable issue is that the issuance of the licence is completely subject to the government's discretion. For instance, s 28(a) provides that requirements of a licence are "determined by the Chief Executive", and its period under s 29(4) is "valid for a period as specific in the licence".

Conditions of the licence, pursuant to s 31(1), are contingent on whatever the Chief Executive "thinks fit to impose", which can be varied or revoked at will. Violating any of these arbitrary conditions is a separate offence subject to two years imprisonment and/or a fine of RM100,000. Also, the licence carries an obligation to produce nearly limitless information "as the Chief Executive may direct" pursuant to s 32(2)(c). While s 53 appears to provide a right of appeal, this appeal is made directly to the minister rather than any independent external review.

Following the above, the Act lacks provisions to address the handling and reviews of complaints against cyber security service providers, such as poor quality of service, misuse of customer data, unethical behaviour or data breach. Specifically, there is no mechanism in the Act to deal with issues concerning membership, such as dealing with a complaint or the establishment of an independent body to deal with complaints which is especially important when the complainant is the Chief Executive or the minister themselves. The absence of these mechanisms may undermine the rights of both cyber security service providers and complainants. Clear mechanisms are crucial for ensuring accountability, safeguarding the rights of complainants and cyber security service providers and upholding professional standards. The Act should emulate statutes like the Legal Profession Act 1976, which has an independent body to deal with disciplinary issues of members.

The only possible recourse under the Act is that the Chief Executive may revoke or suspend the licence if the Chief Executive is satisfied that:

[83] Presentation slides provided at the public dialogue session of the Cyber Security Bill dated November 24, 2023.

(a) the licensee has failed to comply with any conditions of the licence;

(b) the licence has been obtained by fraud or misrepresentation;

(c) a circumstance existed at the time the licence was issued or renewed that the Chief Executive was unaware of, which would have caused the Chief Executive to refuse to issue or renew the licence if the Chief Executive had been aware of the circumstance at that time;

(d) the licensee has ceased to carry on the business in respect of which he is licenced under the Act;

(e) the licensee has been adjudged a bankrupt or has gone into liquidation or is being wound up;

(f) the licensee has been convicted of an offence under the Act or an offence involving fraud, dishonesty or moral turpitude; or

(g) the revocation or suspension is in the interest of the public or national security.[84]

Additionally, the introduction of new standards, practices and severe penalties could impose significant constraints on innovation within the industry. If regulations are overly burdensome, they have the potential to impede the development of new technologies and solutions. This burden is particularly pronounced for smaller technology companies, which may lack the resources necessary to ensure compliance. Consequently, such companies could face challenges in establishing themselves and bringing innovative products or services to market.[85] However, this concern may not be as significant if we consider that MDEC has allocated funds to support new initiatives under Pemangkin. These initiatives enable cyber security service providers to receive tax incentives and other benefits as discussed earlier.

Moreover, trade and business may also face significant financial impacts due to the requirement of licensing for cyber security service providers. As cyber security service providers enhance their offerings to meet higher standards and obtain necessary licences, the costs for these services will likely increase. This could result in higher expenses for businesses seeking to maintain enhanced protection and reliability that licensed, high-quality cyber security services provide.

Furthermore, the high demand for the cyber security professionals, while aiming to ensure industry accountability, also presents disadvantages in dealing with the ongoing war for talent in the cyber security sector. It may exacerbate the existing talent shortage in the industry, with organisations

[84] Cyber Security Act 2024, s 33.
[85] *Hansard*, second reading at the Senate.

competing for a limited pool of skilled professionals. This increased competition drives up salaries and benefits, making it challenging for smaller companies or those with limited budgets to compete with larger firms for talent acquisition.

Besides, the rapid growth in demand for cyber security professionals may outpace the availability of skilled talent, resulting in a widening skills gap within the sector. Organisations may struggle to find professionals with the requisite expertise and experience to meet their cyber security needs, leading to challenges in fulfilling regulatory requirements and maintaining effective cyber security operations. Additionally, the need for specialised skills and certifications may pose challenges in training existing staff or hiring new talent, especially in regions with limited access to cyber security education and training programs.

This highlights the significance for Malaysia to tackle these concerns by collaborating with higher education institutions to integrate cyber security into their curriculum or establish specialised tracks within existing programs. Additionally, there should be a focus on establishing cyber security training facilities to test and train cyber security professionals, as well as investing in research and development to attract and nurture a larger pool of cyber security experts.

Summary of the offences

For ease of reference, the following are offences under the Act:

NCII entity:

- Failure of the NCII entity to comply with the NCII sector lead's request for the provision of information in relation to the NCII (fine not exceeding RM100,000 and/or two years imprisonment or both).[86]
- Failure of the NCII entity to implement the measures, standards and processes as specified in the Code of Practice (fine not exceeding RM500,000 and/or imprisonment for a term not exceeding 10 years).[87]
- Failure of the NCII entity to conduct the cyber risk assessments in accordance with the Code of Practice and directive and carry out an audit (fine not exceeding RM200,000 and/or imprisonment for a term not exceeding three years).[88]

[86] Cyber Security Act 2024, s 20(6).
[87] *Ibid*, s 21(5).
[88] *Ibid*, s 22(7).

- Failure of the NCII entity to submit the audit report (fine not exceeding RM200,000 and/or imprisonment for a term not exceeding three years).[89]

- Failure of the NCII entity to comply with the directive of the Chief Executive 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. (fine not exceeding RM200,000 and/or imprisonment for a term not exceeding three years).[90]

- Failure of the NCII entity to comply with the Chief Executive's direction, which includes failure to re-evaluate the cyber security risk due to the unsatisfied cyber security risk assessment; rectify the audit report that is insufficient; conduct a cyber security risk assessment or carry out an audit due to material change made to the NCII; and conduct an additional cyber security risk assessment or carry out an additional audit, (fine not exceeding RM100,000).[91]

- Failure of the NCII entity to notify cyber security incidents (fine not exceeding RM500,000 and/or imprisonment for a term not exceeding 10 years).[92]

- Failure of the NCII entity to comply with the directions of the Chief Executive for the purpose of the cyber security exercise (fine not exceeding RM100,000).[93]

NCII sector lead:

- Failure of the NCII sector lead to prepare a Code of Practice (fine not exceeding RM100,000).[94]

- Failure of the NCII sector lead to notify the Chief Executive of any information received regarding the provision of information by the NCII entity in relation to the additional NCII or the material change that is made to the NCII (fine not exceeding RM100,000).[95]

[89] *Ibid*, s 22(7).
[90] *Ibid*, s 35(5).
[91] *Ibid*, s 22(8).
[92] *Ibid*, s 23(2).
[93] *Ibid*, s 24(4).
[94] *Ibid*, s 25(6).
[95] *Ibid*, s 20(7).

Other persons:

- Failure of any person to comply with the directions of the Chief Executive to give or produce any information, particulars or document, if the Chief Executive has reasonable grounds to believe that such person possesses any information, particulars, or documents relevant to the performance of the Chief Executive's duties and powers under the Act, or is capable of providing any evidence which the Chief Executive has reasonable grounds to believe is relevant to the performance of their duties and powers under this Act) (fine not exceeding RM200,000 and/or imprisonment for a term not exceeding three years).[96]

- Where the Chief Executive directs any person to produce any document under s 14(1), and the document is not in the custody of that person, that person fails to state, to the best of their knowledge and belief, where the document may be found and identify, to the best of their knowledge and belief, the last person who had custody of the document and to state, to the best of their knowledge and belief, where that last-mentioned person may be found (fine not exceeding RM200,000 and/or imprisonment for a term not exceeding three years).[97]

- Failure of any person directed to give or produce any information, particulars or document or copies of any document under s 14(1) to ensure that the information, particulars or documents or copies of the document given or produced are true, accurate and complete and to provide an express representation to that effect, including a declaration that they are not aware of any other information, particulars or document which would make the information, particulars or document given or produced untrue or misleading (fine not exceeding RM200,000 and/or imprisonment for a term not exceeding three years).[98]

- Any person who provides any cyber security service or advertises, or in any way holds themselves out as a provider of a cyber security service without holding a cyber security service provider licence (fine not exceeding RM500,000 and/or imprisonment for a term not exceeding 10 years).[99]

---

96 *Ibid*, s 14(6).
97 *Ibid*, s 14(7).
98 *Ibid*, s 14(7).
99 *Ibid*, s 27(5).

- Any person who contravenes any conditions of a licence imposed by the Chief Executive. (fine not exceeding RM100,000 and/or imprisonment for a term not exceeding two years).[100]

- Failure of any person to keep and maintain the required records of the cyber security service provider licence under s 32(1), to keep and maintain them in the manner as may be determined by the Chief Executive; to retain for a period of not less than six years from the date the cyber security service was provided; to produce to the Chief Executive at any time as the Chief Executive may direct (fine not exceeding RM100,000 and/or imprisonment for a term not exceeding two years).[101]

- Any person who transferred or assigned the cyber security service provider licence to any other person (fine not exceeding RM200,000 and/or imprisonment for a term not exceeding three years).[102]

- Any person who, without lawful authority, breaks, tampers with or damages the seals placed by the authorised officer due to the impracticability of removing any object, book, account, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter seized by reason of its nature, size and amount, or removes any object, book, account, document, computerised data, signboard, card, letter, pamphlet, leaflet, notice, facility, apparatus, vehicle, equipment, device, thing or matter under seals or attempts to do so (fine not exceeding RM100,000 and/or to imprisonment for a term not exceeding two years).[103]

- Failure of any person to comply with the additional powers[104] of an authorised officer (fine not exceeding RM100,000 and/or imprisonment not exceeding two years).[105]

- Any person who assaults, impedes, obstructs or interferes with, or refuses access to any premises or computerised data to, the Chief Executive or authorised officer in the performance of their duties

100 *Ibid*, s 31(3).
101 *Ibid*, s 32(3).
102 *Ibid*, s 34(2).
103 *Ibid*, s 39(7).
104 *Ibid*, s 51(1) provides that an authorised officer shall, for the purposes of the execution of this Act, have the powers to do all or any of the following: (a) require the production of any computer, book, record, computerised data, document or other article and to inspect, examine and make copies of any of them; (b) require the production of any identification document from any person in relation to any act or offence under this Act; and (c) make such inquiries as may be necessary to ascertain whether the provisions of this Act have been complied with.
105 *Ibid*, s 51(2).

under the Act (fine not exceeding RM100,000 and/or imprisonment for a term not exceeding two years).[106]

- Any member of the NCSC, the Chief Executive or any authorised officer, whether during or after his tenure of office or employment, disclose any information obtained by him in the course of his duties except for any of the purposes of the Act or for the purposes of any civil or criminal proceedings under any written law or where otherwise authorised by the NCSC (fine not exceeding RM100,000 and/or imprisonment for a term not exceeding two years).[107]

Compoundable offence

Notably, s 60 of the Act provides that the Minister may make regulations prescribing any offence under the Act as an offence which may be compounded, and the method and procedure for compounding such offence.

The Cyber Security (Compounding of Offences) Regulations 2024 lists out the six offences under the Act which are being capable of being compounded (if consented to by the Public Prosecutor in writing at the material time). These include:

(i) Section 20(6): Failure of the NCII entity to provide information relating to its NCII.

(ii) Section 20(7): Failure of the NCII sector lead to notify the Chief Executive of any information received regarding the provision of information by the NCII entity in relation to the additional NCII or the material change that is made to the NCII.

(iii) Sections 22(7) and 22(8): Failure of the NCII entity to conduct cyber security risk assessment and audit (and subsequent failure to submit the reports to the Chief Executive of NACSA) as well as a NCII entity's failure to comply with directions to the NCII entity arising from the findings in such reports.

(iv) Section 24(4): Failure of the NCII entity to comply with the directions of the Chief Executive of NACSA in relation to cyber security exercises.

(v) Section 32(3): Failure of any person to keep and maintain the required records of the cyber security service provider licence under s 32(1), to keep and maintain them in the manner as may be determined by the Chief Executive; to retain for a period of not less than six years from

106 *Ibid*, s 52.
107 *Ibid*, s 55(2).

the date the cyber security service was provided; to produce to the Chief Executive at any time as the Chief Executive may direct.

Section 58 provides that where any person who commits an offence under the Act is a:

(i) company;

(ii) limited liability partnership;

(iii) firm;

(iv) society; or

(iv) other body of persons i.e. a person who at the time of the commission of the offence was a director, compliance officer, partner, manager, secretary or other similar officer of the company, limited liability partnership, firm, society or other body of persons or was purporting to act in the capacity or was in any manner or to any extent responsible for the management of any of the affairs of the company, limited liability partnership, firm, society or other body of persons or was assisting in its management –

(a) may be charged severally or jointly in the same proceedings with the company, limited liability partnership, firm, society or other body of persons; and

(b) if the company, limited liability partnership, firm, society or other body of persons is found guilty of the offence, shall be deemed to be guilty of the offence and shall be liable to the same punishment or penalty as an individual unless, having regard to the nature of his functions in that capacity and to all circumstances, he proves –

(i) that the offence was committed without his knowledge; and

(ii) that the offence was committed without his consent or connivance and that he had taken all reasonable precautions and exercised due diligence to prevent the commission of the offence.

Section 59 provides that where any person would be liable to any punishment or penalty for any act, omission, neglect or default committed:

(a) by that person's employee in the course of his employment;

(b) by that person's agent when acting on behalf of that person; or

(c) by the employee of that person's agent when acting in the course of his employment with that person's agent or otherwise on behalf that person's agent acting on behalf of that person,

that person shall be liable to the same punishment or penalty for every such act, omission, neglect or default of that person's employee or agent, or of the employee of that person's agent.

Closing

Overall, the implementation of the Act is a timely and positive step for Malaysia in the face of increasing and evolving cyber threats. The Act has the potential to address existing legal gaps and enhance cyber defence mechanisms. It marks a significant milestone in protecting the NCII amidst a rapidly changing cyber landscape. However, given the presence of certain uncertainties and shortcomings, it is hoped that such uncertainties and shortcomings can be resolved through the implementation of regulations and guidelines. The Act must balance protecting the NCII with creating an environment that encourages businesses and protects the rights of the parties involved.

Given the potential financial constraints that NCII entities may encounter while adhering to the provisions of the Act, it is imperative for the government to extend support in various forms, such as tax benefits, incentives, grants or subsidies, and guidance, to alleviate their burden and foster an environment conducive to innovation and digital advancement. Also, regarding the implementation of the Code of Practice, it is important for the government to plan an interim period for industry consultation and feedback, to make necessary adjustments and responses to ensure its effectiveness. It is paramount to ensure that any legislative or policy measures implemented within the cyber environment do not inadvertently impede innovation or hinder the growth of the digital economy.

Despite the challenges posed by these changes, organisations can mitigate their concerns by building robust internal cyber security capabilities. Due to the negative publicity and financial risks of cyberattacks, being prepared for cyber security is becoming essential for businesses. Organisations should be prepared and anticipate that they will be designated as an NCII entity and take proactive measures to ensure they are ready to comply with the requirements of the Act once it is enforced. This involves ensuring that they have the necessary processes, structures, and personnel to manage cyber security issues and comply with regulations.

Essential components of these capabilities include:

(1) strengthening their cyber security;

(2) reviewing, updating and re-evaluating their current cyber security policies and procedures. If they lack such policies and procedures,

they should consult with legal and professional experts to create them. The creation of Codes of Practice is not a new area, as many other legislations, such as the Communications and Multimedia Act 1998 and the Personal Data Protection Act 2010, require the creation of such codes;

(3) undertaking risk assessment measures;

(4) developing and implementing effective risk management strategies;

(5) creating cyber security incident response plans;

(6) obtaining the necessary cyber insurance;

(7) performing threat intelligence analysis to anticipate future threats;

(8) establishing cyber security incident handling and digital forensics;

(9) implementing cyber security network defence and penetration testing; and

(10) fostering cyber security awareness of the various types and sophistication of cyberattacks, among employees and third-party contractors, by organising regular and consistent cyber security training or tabletop simulations of cyberattacks.

With respect to cyber insurance, while increased costs are inevitable, it is crucial as it could soften the blow of the consequences of a cyber security breach or non-compliance with the Act. Especially for industries operating on narrow profit margins, these expenditures could determine whether a year ends in profit or loss. From an insurance standpoint, regulatory protection within a cyber policy covers expenses related to legal defence and investigation in the event of regulatory inquiries or claims arising from cyber incidents or mishandling of such events. Other insurable aspects within a cyber policy encompass expenses for breach response, data administration investigation and regulatory investigation expenses. The requirement for mandatory reporting of cyber incidents[108] can help insurers more accurately price risks and provide better protection.

Organisations should grasp their specific risk exposure when evaluating cyber insurance, especially given the lack of standardised forms in the Asian cyber insurance market. Consequently, policies vary in their coverage. Even subtle variations in language can significantly affect the extent of coverage available.

Due to the widespread use of artificial intelligence and its growing exploitation by threat actors for cyber attacks, it is essential for everyone in

[108] *Ibid*, s 23.

the company to be aware of cyber threats and attacks. This is particularly important because the majority of cyber security incidents are often caused by human susceptibility, carelessness or accidents.