LH AG ADVOCATES AND SOLICITORS

LHAG | TECH

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

The Duties and Responsibilities under the Cyber Security Act 2024

CYBERSECURITY SERIES
OCTOBER 2024

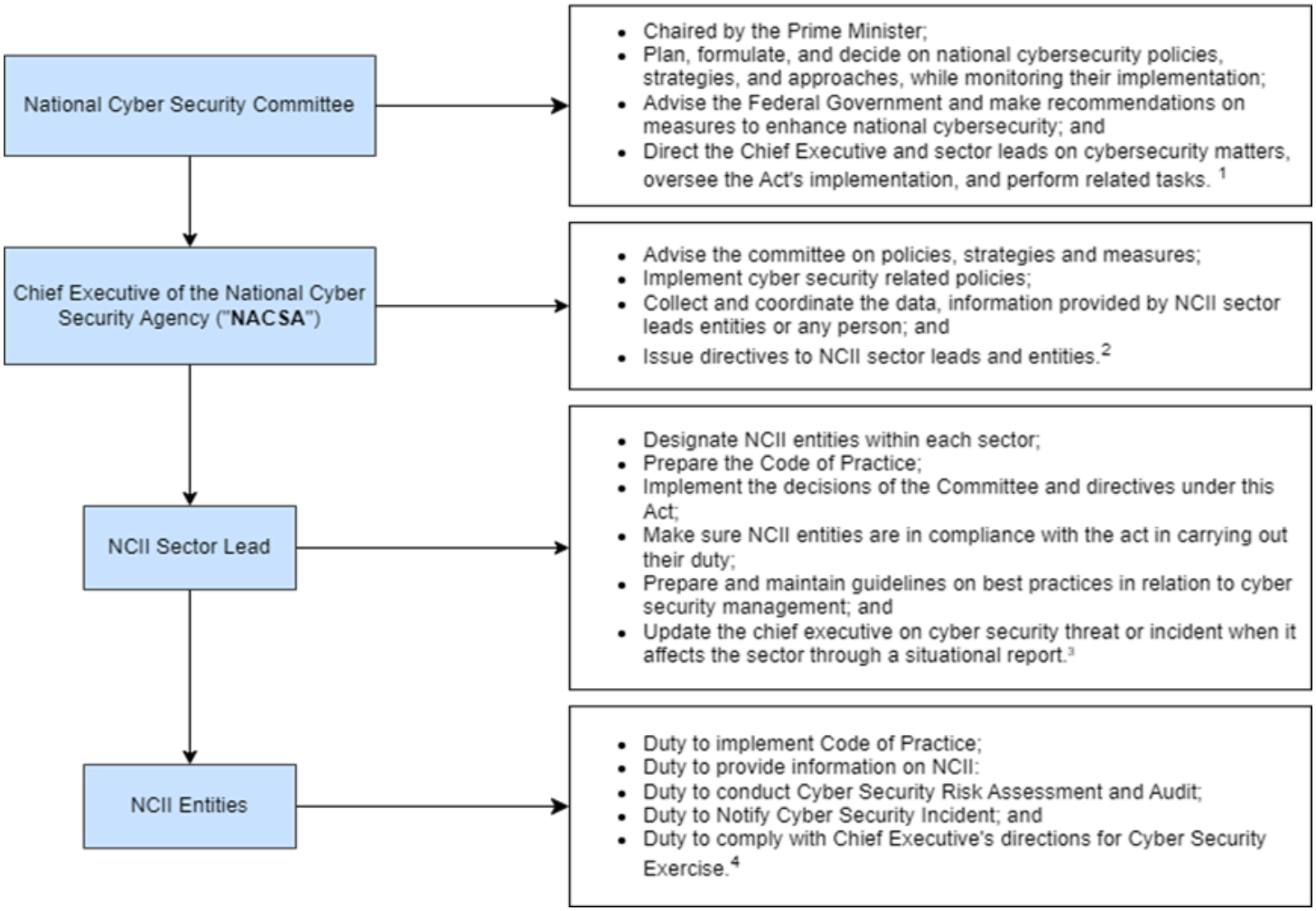
VIJAY KUMAR
Partner
Corporate Disputes | TMT
vkg@lh-ag.com

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

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

In our previous article in this Cybersecurity Series, we explored the latest developments in Malaysia's cybersecurity framework and their impact on the regulated entities. Building on that, this article will explore the key duties and responsibilities under the Act and its regulations.

Summary of the Key Duties and Responsibilities



Given the critical role NCII entities play in safeguarding national cybersecurity, it is essential that they fully comply with the duties and responsibilities under the Act and Regulations. With the increasing cybersecurity threats, NCII entities are presumptively the most likely targets of such attacks. In 2023, ransomware attacks in Malaysia doubled, with 85.2% involving data exfiltration, highlighting the escalating risks in the cybersecurity landscape. Below, we provide an outline of the obligations imposed on NCII Entities under the Act and its Regulations:

1. Duty to Provide Information on NCII:

Upon request by the NCII Sector Lead, the NCII Entity must provide relevant information about its NCII. If the NCII Entity acquires or has control over any new computer or system that is a NCII, it must notify the Sector Lead. Additionally, any material changes made to the design, configuration, security or operation of the NCII Entity must be report to the Sector Lead. [5]

2. Duty to Implement Code of Practice:

The NCII Entity must implement the measures, standards, and processes specified in the code of practice or adopt alternative methods to ensure the cybersecurity of its NCII. Although the relevant codes of practice are still under development, NCII Entities should consider adopting the standards under other international cybersecurity frameworks. [6]

3. Duty to Conduct Cyber Security Risk Assessment and Audit:

The NCII Entity shall conduct a cybersecurity risk assessment on its NCII at least once a year, and commission an audit by an auditor approved by the Chief Executive at least every two years. Following these assessments, the NCII Entity must submit the cybersecurity risk assessment report or audit report to the Chief Executive within 30 days of completion. [7]

4. Duty to Notify Cyber Security Incident:

If an NCII Entity becomes aware that a cyber security incident has or might have occurred in respect of its NCII, it shall report the incident immediately through the National Cyber Coordination and Command Centre System (NC4S). [8]

5. Duty to Comply with Chief Executive's Directions for Cyber Security Exercise:

If the Chief Executive directs to conduct a cybersecurity exercise to assess the preparedness of any NCII Entity in handling cybersecurity threats or incidents, the NCII Entity is obligated to follow all instructions given by the Chief Executive. [9]

It is undisputable that NCII entities play a critical role in safeguarding national cybersecurity. Although the Act and its regulations are still in their early stages of implementation, rapid developments are expected. In this regard, we note that the Sector Leads have already been appointed, we can expect that the NCII entities are likely to be appointed fairly soon.

---

[1] Cyber Security Act 2024, s.6
[2] Cyber Security Act 2024, s.10
[3] Cyber Security Act 2024, s.16
[4] Cyber Security Act 2024, s.18
[5] Cyber Security Act 2024, s.20
[6] Cyber Security Act 2024, s.21
[7] Cyber Security Act 2024, s.22
[8] Cyber Security Act 2024, s.23 & 35
[9] Cyber Security Act 2024, s.24

The NCII Entities are advised to take proactive steps now to align with the Act. Guidance can be obtained can be drawn from our neighbour Singapore, where a Code of Practice is already in place. Considering the similarity of the Act and the Singapore Cybersecurity Act 2018, it is reasonable to expect a comparable Code of Practice to be introduced in Malaysia.

Given the circumstances, the NCII entities should proactively budget for increased operational costs to comply with their duties and responsibilities under the Act. This will likely entail investing in advanced cybersecurity technologies and hiring qualified personnel to strengthen their cybersecurity teams. NCII entities can better position themselves to meet future obligations and mitigate cybersecurity risks effectively.

In our next article, we will closely examine the procedural steps outlined in the Act and its regulations for NCII entities to respond to cybersecurity attacks. For further assistance on any legal matters, please do not hesitate to contact any of the authors below.