# Take5 for business

Volume 13 Issue 3 - 8 May 2024

## Malaysia: Cyber Security Bill 2024

Enhancing and safeguarding Malaysia's cybersecurity landscape

EY
Building a better working world

# Safeguarding Malaysia's cybersecurity infrastructure

On March 27, 2024, the Malaysian Parliament approved the Cyber Security Bill 2024. The Bill, designed to improve and protect the cybersecurity environment in Malaysia, introduces requirements to entities within the National Critical Information Infrastructure (NCII) sectors to comply with specific standards and measures, as well as processes when handling cybersecurity incidents.

Significantly, the Bill introduces a regulatory framework for the eleven NCII sectors. In addition, NCII sector leads are empowered to designate any entity which owns or operates any NCII as a designated NCII entity, and prepare Codes of Practice.

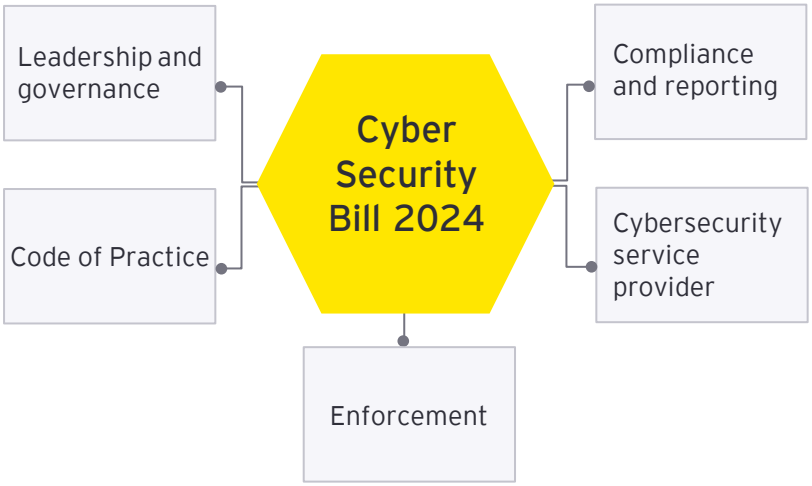
In addition to the governance and Code of Practice aspects, the Bill's scope extends to:

- Compliance and reporting;
- Licensing of cybersecurity service providers; and
- Enforcement and penalties.

> "In a market of accelerating complex change, the Cyber Security Bill 2024 marks a significant milestone in safeguarding our nation's critical infrastructure.
>
> As we move forward, it is crucial to ensure that there is sufficient industry consultation and collaboration on the Codes of Practice and their implementation.

**Jason Yuen**
Malaysia Cybersecurity Leader, Ernst & Young Consulting Sdn Bhd

## Cyber Security Bill 2024: Regulatory framework




**Eleven NCII sectors**

1. Government
2. Banking and finance
3. Transportation
4. Defense and national security
5. Information, communications and digital
6. Healthcare services
7. Water, sewage and waste management
8. Energy
9. Agriculture and plantation
10. Trade, industry and economy
11. Science, technology and innovation

# Applicability of the Bill and governing bodies

### Extraterritoriality

The Bill is intended to have extraterritorial application and shall apply to any person, irrespective of his or her nationality or citizenship, and shall have effect outside, as well as within Malaysia. The Federal Government and State Governments are also subject to the Bill.

### National Cyber Security Committee and Chief Executive's powers

The Bill establishes a 13-member National Cyber Security Committee which shall be chaired by the Prime Minister of Malaysia. Its primary function is to advise and provide recommendations to the Federal Government to strengthen cybersecurity, oversee the implementation of the Bill (when it comes into force) and give directions to the Chief Executive of the National Cyber Security Agency ("Chief Executive") and the NCII sector leads on matters relating to national cybersecurity.

The Chief Executive, in turn, is empowered under the Bill to establish the National Cyber Coordination and Command Centre system for the purpose of dealing with cybersecurity threats and cybersecurity incidents and issue directives as necessary for the purpose of ensuring compliance with the Bill.

### Designated NCII entities are subject to several obligations including:

Providing information to the relevant NCII sector lead when requested

Conducting cybersecurity risk assessments and audits

Complying with any relevant Codes of Practice issued by the NCII sector leads

Notifying the relevant NCII sector lead and the Chief Executive when there is a cybersecurity incident

Note:

According to the Bill, the Chief Executive holds the responsibility of executing and monitoring the application of national cybersecurity policies, strategies, and measures as directed by the Committee or the Federal Government.

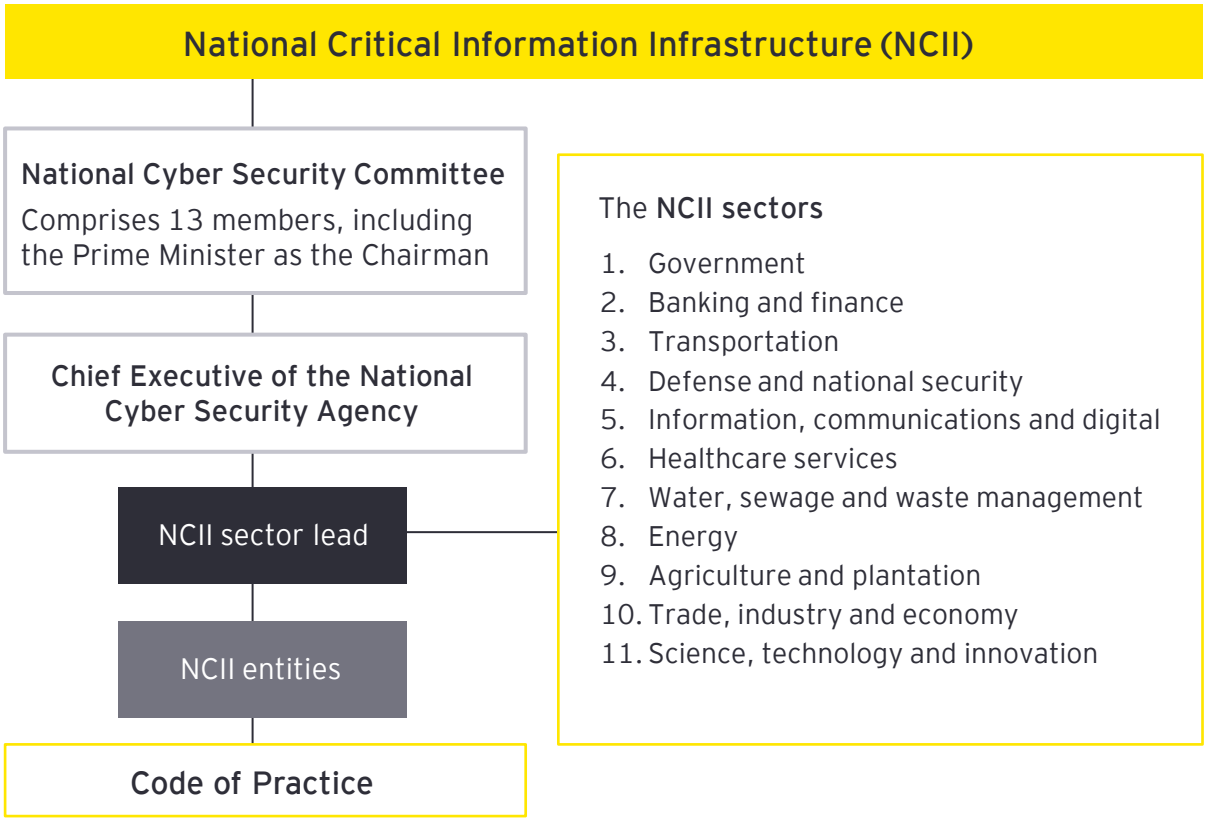
The Chief Executive is also charged with monitoring their execution by NCII sector leaders, entities, and government institutions. Furthermore, the Chief Executive is given special enforcement powers, including the authority to probe cybersecurity incidents within NCII entities

Source: Cyber Security Bill 2024, 22 March 2024, Malaysia

# Governance and Code of Practice

In strengthening cybersecurity governance in Malaysia, strong industry involvement in the cybersecurity landscape is required, including the formation of the NCII Council and sub-committees as well as the participation of industry experts from large to small-medium enterprises (SMEs) with strong proven experience across relevant sectors.

During the development and implementation of the Code of Practice, it is also crucial for the NCII to plan an interim implementation period for seamless industry consultative and feedback processes.




| | |
|---|---|
| **Implementation of the Code of Practice** | Set measures, standards and processes |
| **Provision of information** | Provide Information relating to the NCII-owned entity or one operated by the said NCII entity |
| **Cybersecurity risk assessment** | Conduct and submit a cybersecurity risk assessment in accordance with the Code of Practice |
| **Incident-reporting processes** | Conduct an audit with an auditor approved by the Chief Executive |
| **Compliance and auditing** | Report to the Chief Executive and the NCII sector lead |
| **Cybersecurity exercises** | Comply with the Chief Executive's directions upon receipt of a notice-in-writing from the Chief Executive |

Source: Cyber Security Bill 2024, 22 March 2024, Malaysia

# Compliance, reporting and licensing

To mitigate the prevalence of cybersecurity incidents in Malaysia, the requirements and considerations under compliance and licensing for cybersecurity service providers include:

### Compliance and reporting

- In the event of cybersecurity incidents, NCII entities are required to report to the Chief Executive and the NCII sector lead; and
- NCII entities need to establish a compulsory incident reporting process e.g., for cyberattacks.

### Licensing for cybersecurity service providers

- Cybersecurity providers are required to obtain a non-assignable or transferable license to provide a cybersecurity service; and
- The Chief Executive should consider expanding the licensing framework to include a Code of Practice for the service providers, particularly on the qualifications or requirements to be service providers and the proper process to address complaints, arbitrations and resolutions.

Source: Cyber Security Bill 2024, 22 March 2024, Malaysia

# Enforcement and penalties

To monitor the enforcement of the Bill, the Chief Executive should develop a proper standard of proof that includes the internal processes and controls needed for companies, and the policies and documentations required.

The designated NCII entities must also ensure their compliance with any Codes of Practice issued by the relevant NCII sector to avoid any legal penalties.

| | Obligations | Legal penalties |
|---|---|---|
| 1 | Compliance with the Code of Practice | In the event a NCII entity fails to comply with the requirements under a Code of Practice, it may be liable to a fine not exceeding RM500,000 or imprisonment for a term not exceeding 10 years, or both. |
| 2 | Provision of information in relation to the NCII | ► Failure by the NCII entity to comply with the NCII Sector lead's request will result in a fine not exceeding RM100,000 or imprisonment for a term not exceeding two years, or both.<br>► NCII Sector leads that fail to report the same, upon receipt of the information, to the Chief Executive may be liable to a fine not exceeding RM100,000. |
| 3 | Conduct of a cybersecurity risk assessment | ► NCII entities that fail to conduct cybersecurity risk assessments may be found liable to a fine not exceeding RM200,000 or imprisonment for a term not exceeding three years, or both.<br>► Failure to comply with the Chief Executive's direction will result in a fine not exceeding RM100,000. |
| 4 | Audit | ► NCII entities are required to carry out an audit by an auditor approved by the Chief Executive to determine the compliance of the NCII entity with the Bill and submit the audit report to the Chief Executive<br>► Inadequate audit reports submitted to the Chief Executive necessitate rectification under the Chief Executive's directives.<br>► Failure to submit the audit report will result in a fine not exceeding RM200,000 or imprisonment for a term not exceeding three years, or both, while failure to comply with the Chief Executive's direction will result in a fine not exceeding RM100,000 |
| 5 | Reporting | Failure to report a cybersecurity incident may attract a fine of not more than RM500,000 or imprisonment for a term not exceeding 10 years or both. |
| 6 | Cybersecurity exercise | NCII entities are required to comply with the Chief Executive's directions, upon receipt of a notice in writing from the Chief Executive of his intention to conduct a cybersecurity exercise with respect to the NCII.<br>In the event an NCII entity fails to comply with the directions of the Chief Executive, it may be liable to a fine not exceeding RM100,000. |
| 7 | Licensing of the cybersecurity service provider | Any person or entity without a license, that provides cybersecurity services or holds itself out as a provider of cybersecurity services, shall be liable to a fine not exceeding RM500,000 or imprisonment for a term not exceeding 10 years, or both. |

Source: Cyber Security Bill 2024, 22 March 2024, Malaysia

# Key actions

With the rapid digital transformation in various industries and sectors catalyzed by artificial intelligence (AI) and other technological innovations, the heightening cybersecurity threats require businesses, regardless of their size, to step-up cybersecurity actions in order to manage current and emerging risks. Among the key actions to consider include:

1. Anticipating a higher level of cybersecurity governance and compliance in view of the operationalization of the Code of Practice, including its potential spillover to non-critical information infrastructure.
2. Expecting higher overhead costs with the additional processes and technologies in key areas such as risk assessment, security monitoring, compliance and cyber simulations.
3. Preparing for increased costs with the higher quality of cybersecurity services in relation to the licensing of service providers.
4. Dealing with the ongoing war for talent for cybersecurity professionals and skills as a result of higher demand growth.
5. Adopting leading technology solutions, automation and AI solutions to step up capabilities and keep pace with evolving threats.

> “
>
> The need for rapid transformation often results in businesses overlooking cybersecurity.
>
> The risk of moving forward without addressing gaps, as businesses maintain new working practices in an increasingly complex global economy, is increasingly high. The cybersecurity incidents happening to-date underscore how critical immediate action is.

**Jaco Benadie**
EY Asean Cybersecurity Energy Leader and OT Cybersecurity Competency Lead

Source: EY analysis

# EY contacts

**Dato' Abdul Rauf Rashid**
Malaysia Managing Partner,
Ernst & Young PLT

abdul-rauf.rashid@my.ey.com

**Chow Sang Hoe**
Malaysia Consulting Leader,
Ernst & Young Consulting Sdn Bhd

sang-hoe.chow@my.ey.com

**Jason Yuen**
Malaysia Cybersecurity Leader,
Ernst & Young Consulting Sdn Bhd

jason.yuen@my.ey.com

**Jaco Benadie**
EY Asean Cybersecurity Energy Leader
and OT Cybersecurity Competency Lead

jaco.benadie@my.ey.com

**EY** | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.



APAC no. 07010464
ED None



**ey.com/en_my**