Traditional Values, Modern Approach™
Issue #13 November 2025

EVOLVING REGULATORY LANDSCAPE FOR DIGITAL & TECH AND THE LATEST CYBERSECURITY ACT IN MALAYSIA

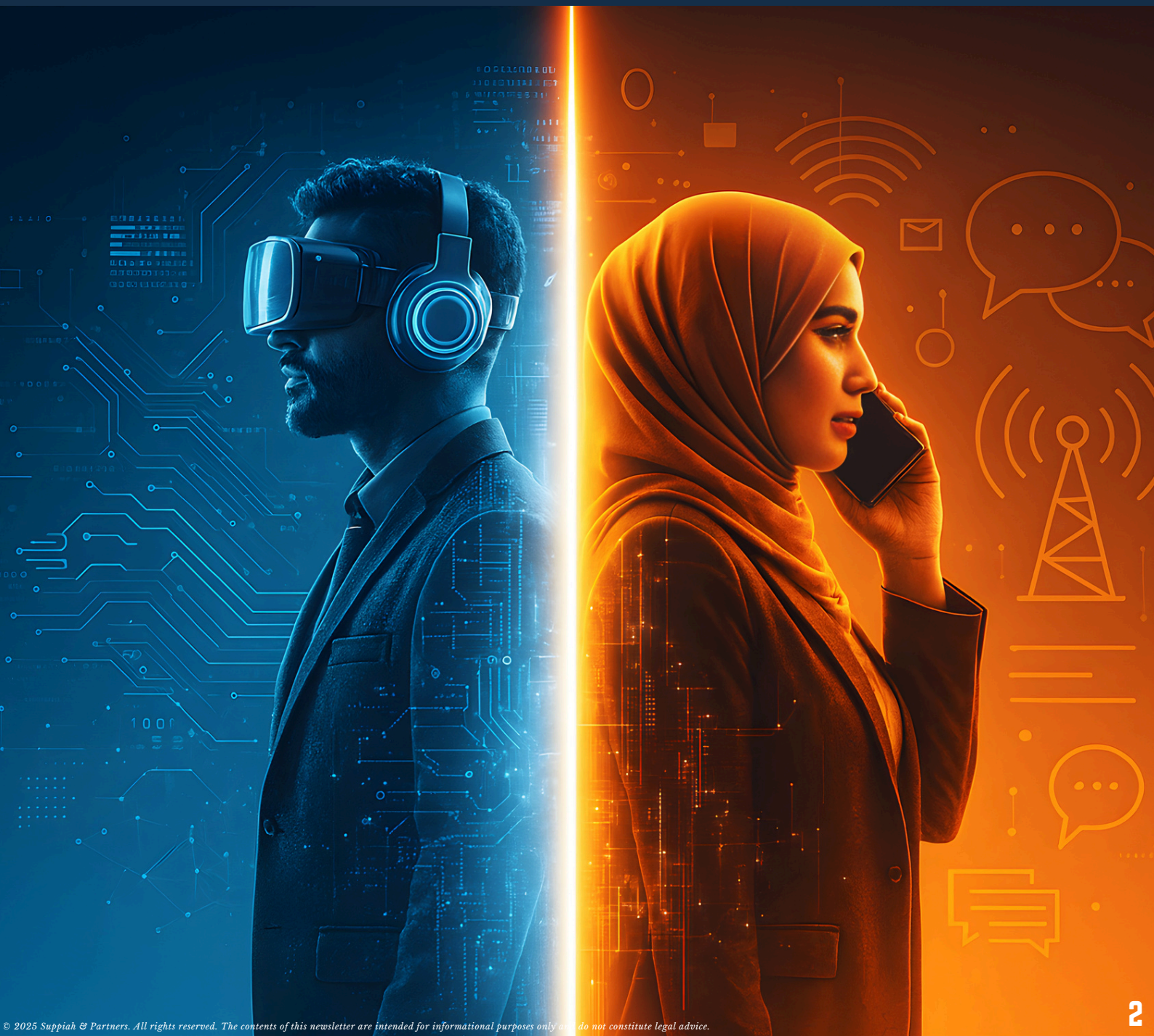
By Thulasy Suppiah, Managing Partner of Suppiah & Partners
& Adjunct Professor Murugason R. Thangarathnam,Chief Executive Officer of Novem CS

INTRODUCTION

Malaysia has been resolutely updating its digital and technology regulations with forward-looking policies. They signify the nation's aspirations to strengthen areas such as online safety, cybersecurity and data protection and governance, and to address the complex and global nature of the digital environment. Given the severity of potential harms, self-regulation by tech companies is insufficient to protect individuals and maintain trust. By strengthening data governance and establishing frameworks like the National Guidelines on AI Governance & Ethics, Malaysia is actively working to build a trusted and secure digital ecosystem for both consumers and businesses.

Several important developments have transpired in Malaysia's digital regulatory landscape especially in the last two years, indicative of the government's strong commitment to cultivate a safe digital ecosystem. For businesses operating or looking to operate in Malaysia, especially businesses in the telecommunications, technology, information security, or other infrastructure sectors, let us hold your hands and take you through these important developments.

First, the Ministry of Communications and Digital was separated into two ministries – the Ministry of Digital and the Ministry of Communications. The separation in 2023, clarified mandates for communications regulations versus digital governance. The Ministry of Digital now oversees the Personal Data Protection Department (PDPD) and, through its Minister Gobind Singh Deo, has proposed a Data Commission to execute the Data Sharing Act.

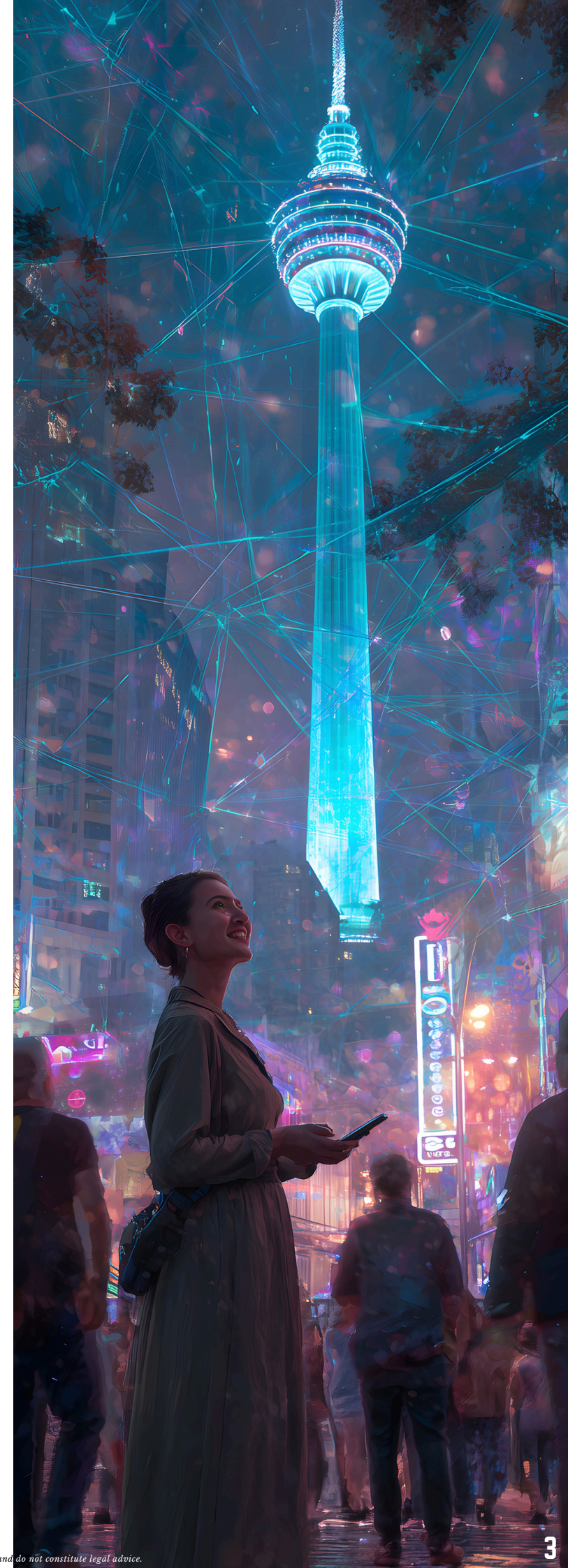


Then in August 2024, The Cyber Security Act 2024 (Act 854) came into force. This is a landmark piece of legislation in Malaysia aimed at strengthening the nation's cyber defences and resilience against evolving cyber threats.

As of June 2025, major amendments to the Personal Data Protection Act (PDPA) took effect. The amendments include new requirements for mandatory data breach notification, the right to data portability, and the appointment of a Data Protection Officer (DPO). Businesses acting as data processors now face direct security obligations, while maximum fines for non-compliance have more than tripled to RM 1,000,000.

Malaysia was the first ASEAN Member State to enact a comprehensive data protection legislation in 2010 but the recent amendments align Malaysia's data protection standards more closely with influential international frameworks like the EU's GDPR (General Data Protection Regulation).

This paper aims to breakdown the key components and implications of the Cyber Security Act 2024 (CSA), vital to protect our digital environment and earn the trust of all Malaysians.



OVERVIEW OF MALAYSIA'S LATEST CYBERSECURITY ACT

Key provisions and scope

The CSA 2024 establishes Malaysia's digital defence framework by certifying the National Cyber Security Committee (NACSA) as the national lead agency with legislative power to ensure the effective implementation of this Act. It outlines the duties and powers of the Chief Executive of NACSA, as well as the functions and duties of the National Critical Information Infrastructure (NCII) sector leads and NCII entities.

The NCII is essentially the central nervous system of a country—the most vital computer systems, networks, and data that keep essential services like banking, electricity, telecommunications, and agriculture, running - the stuff that absolutely must work for society to function normally. It is the information and the digital technology that is so important to a nation that if it were to be shut down, destroyed, or seriously damaged, it would have a devastating impact on national security, the economy, or public health and safety.

The CSA sets the mandatory cybersecurity standards for NCII operators, and creates a licensing regime for cybersecurity service providers to regulate incident response and practice across the country. The Act also has extra-territorial application, to the extent that it imposes requirements for any NCII that "is wholly or partly in Malaysia".

Objectives and regulatory framework

The primary goal of the CSA is to ensure a secure, trusted, and resilient cyberspace in Malaysia and to safeguard critical national functions. Its key objectives can be broken down as such:

- To enhance Malaysia's overall cyber defence capabilities and resilience against emerging and sophisticated cyber threats.

- To establish a comprehensive legislative framework for the protection of the National Critical Information Infrastructure (NCII)

- To establish the necessary governmental structures and legal powers to oversee national cybersecurity policies, with the NACSA as the lead implementing and enforcement agency.

- To regulate the quality and integrity of the cybersecurity services provided in Malaysia through a mandatory licensing regime.

- To institute clear, mandatory standards for managing cyber threats and reporting cyber security incidents, particularly those affecting the NCII.

The CSA identifies the 11 sectors designated as NCII sectors, and mandates strict compliance for organisations operating within them.

These sectors, listed below, are now legally required to enhance their cyber resilience or face penalties:

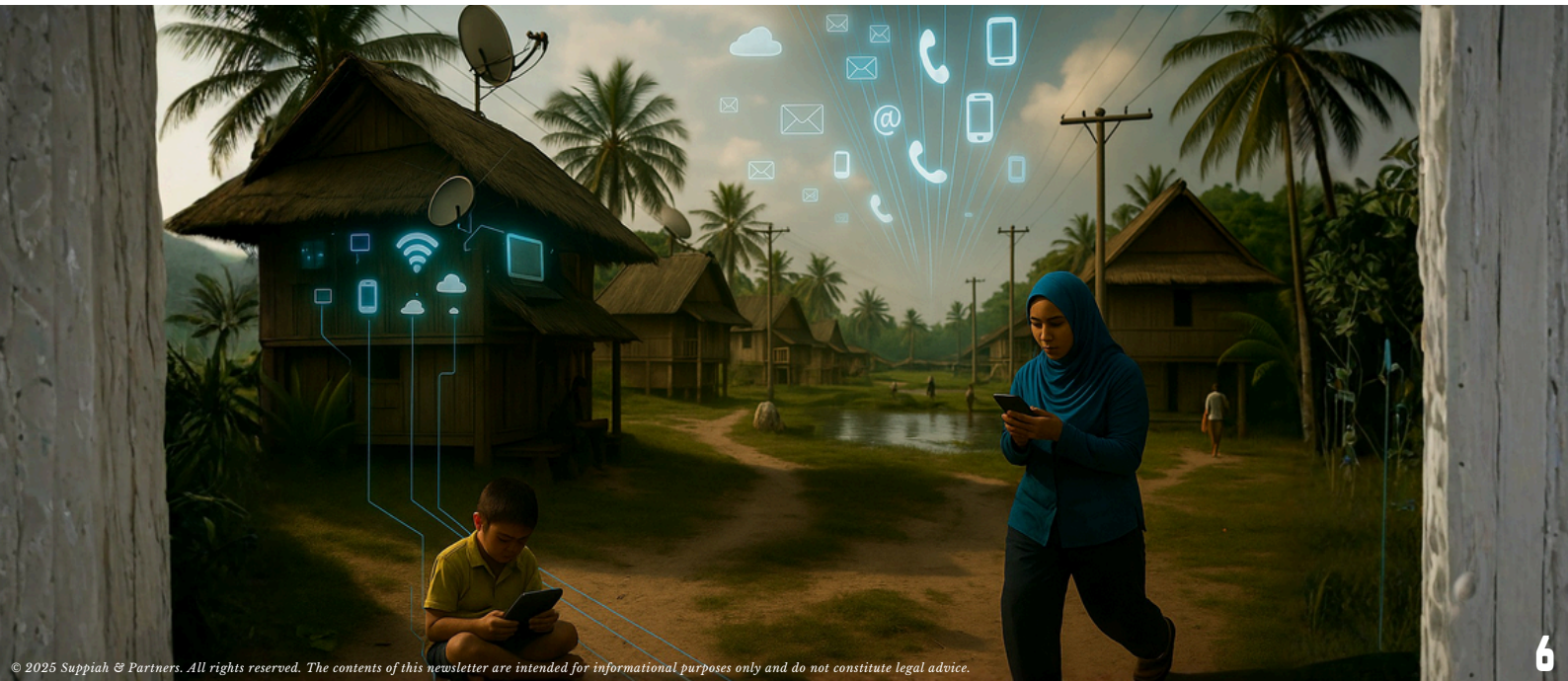
- Agriculture & Plantation
- Banking & Finance
- Defence & National Security
- Energy
- Government
- Healthcare Services
- Information (Communication & Digital)
- Science, Technology, & Innovation
- Trade, Industry, & Economy
- Transportation
- Water, Sewage, & Waste Management

To manage the 11 NCII sectors, the Act allows the Minister to appoint multiple NCII Leads per sector for flexibility. All appointed Leads will be publicly listed on the NACSA website.

Enforcement mechanisms and penalties

The Act applies to licensed cybersecurity service providers (CSSPs) that are designated as NCII entities and the penalties are substantial, including large fines and long imprisonment terms for noncompliance. The key mechanisms used to ensure compliance and investigate violations are:

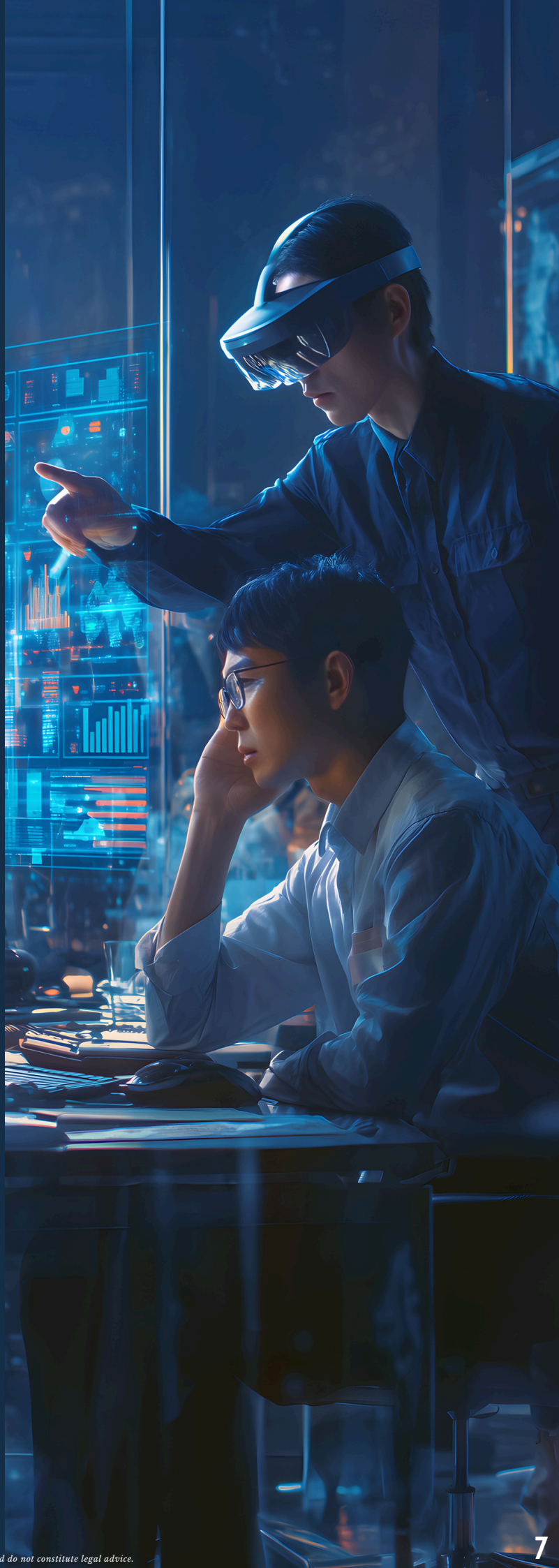
Duty to Provide Information Relating to NCII: NCII Entities must provide all requested NCII information to the Sector Lead, automatically report the acquisition of any new NCII, and notify the Lead of any material changes to the NCII's design, configuration, security, or operation. Failure to comply with any of these duties carries a penalty of up to RM100,000 fine, two years imprisonment, or both.



Duty to Implement the Code of Practice: NCII Entities must implement the measures, standards, and processes specified in the Code of Practice. However, they may use alternative measures if they prove an equal or higher level of NCII protection. Failure to comply can result in a fine up to RM500,000, imprisonment up to ten years, or both.

Duty to Conduct Cybersecurity Risk Assessment and Audit: NCII Entities must conduct mandatory cybersecurity risk assessments (at least annually) and audits (at least once every two years). The results must be submitted to the Chief Executive. Failure to conduct these assessments or submit the reports can lead to a fine of up to RM200,000 or imprisonment for a term not exceeding three years, or both.

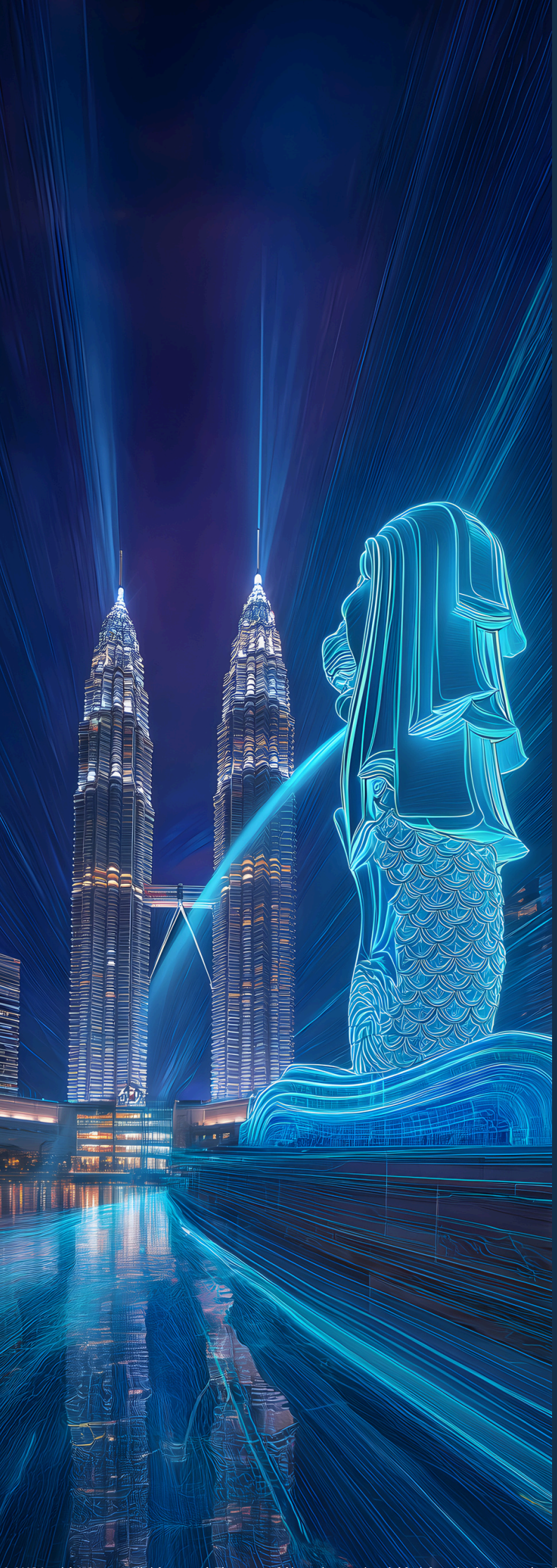
Duty to Notify Cyber Security Incidents: NCII Entities have a strict legal duty to immediately report cyber security incidents to the Chief Executive and their Sector Lead (with a detailed report required within a short timeframe, typically 6 hours for initial details). The initial notification should describe the cybersecurity incident, its severity, and the method of discovery. A full report must be submitted within 14 days, including details such as the number of hosts affected, information on the cybersecurity threat actor, and the incident's impact. Noncompliance invites penalties of up RM500,000 or imprisonment for a term not exceeding ten years, or both.



Cybersecurity Incident Response Directive: Upon receiving a notification of a cybersecurity incident from an NCII Entity, the Chief Executive will investigate and may issue a directive on necessary measures to respond to or recover from the incident. The term “directive” underscores the importance of compliance. Failure to adhere to these directives may result in a fine of up to RM200,000 ringgit or imprisonment for a term not exceeding three years, or both.

Licensing: The CSA establishes a licensing regime for individuals and entities providing prescribed cybersecurity services. There are currently two categories of prescribed cyber security services: (i) managed security operation centre monitoring services; and (ii) penetration testing services. To obtain a licence, an application must be made to the Chief Executive with a prescribed fee and required documents (including qualifications and ID). Applicants must meet prerequisites set by the Chief Executive and have no convictions for fraud, dishonesty, or moral turpitude. The Chief Executive can approve the licence (with variable conditions) or refuse it (stating the grounds). Operating without a required licence is an offence. Providing or advertising services without a licence will incur a fine of up to RM500,000 or imprisonment up to ten years, or both. A fine up to RM200,000 or imprisonment up to 3 years, or both will be imposed for a breach of license conditions.

A broad extra-territorial scope: The CSA’s authority extends beyond Malaysia's physical borders. The extraterritorial reach is particularly important for foreign companies that operate services or infrastructure in Malaysia, especially those designated as NCII Entities. If a foreign multinational company's Malaysian subsidiary owns or operates NCII in Malaysia, the foreign parent company and its personnel can potentially face legal consequences under the CSA for offences or non-compliance related to that Malaysian NCII. Foreign-based CSSPs whose services (like managed security or penetration testing) affect NCII within Malaysia must also comply with the Act's licensing requirements and standards.



COMPARATIVE ANALYSIS WITH SINGAPORE

Malaysia's Cyber Security Act 2024 (CSA) is fundamentally like Singapore's Cybersecurity Act 2018 (SG CA) – both are national laws designed to protect critical digital infrastructure. Both Acts establish a dedicated national agency with primary authority: the National Cyber Security Agency (NACSA) in Malaysia and the Cyber Security Agency in Singapore

While both Acts are primarily designed to protect infrastructure with critical information that is the NCII in Malaysia and the Critical Information Infrastructure (CII) in Singapore, the main differences lie in the severity of penalties, scope of regulation, and specific reporting requirements.

Malaysia’s penalties for non-compliance are generally harsher. For instance, our maximum fine is up to RM500, 000 and/or imprisonment up to 10 years for serious noncompliance (e.g., failure to report an incident or implement the Code of Practice). Singapore’s SG CA 2018 was less severe but its 2024 amendments have increased penalties, allowing for civil penalties up to S$500,000 (RM1,626,160) or 10 per cent of annual turnover for the entity, whichever is greater. However, the maximum penalty for certain core breaches (like failing an audit) in Singapore, is generally lower than Malaysia's for similar offences.

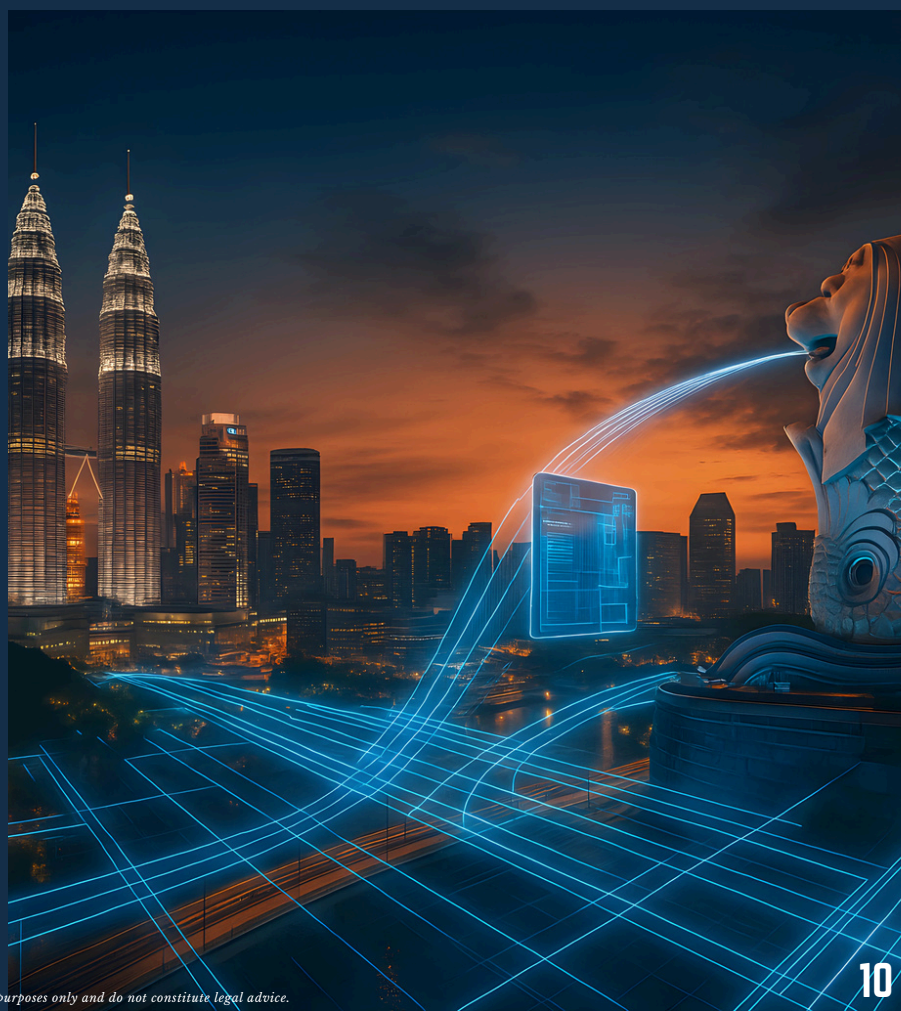
Malaysia’s CSA also primarily focuses on criminal penalties (fines and/or imprisonment) for non-compliance while Singapore employs a flexible mix of civil and criminal penalties. The Cybersecurity Agency can pursue civil penalties instead of criminal ones for certain breaches.

In terms of the scope of incidence reporting, the CSA primarily focuses on incidents directly affecting the NCII entity itself. Singapore's SG CA has a broader scope following its 2024 amendments, requiring CII owners to report incidents involving their third-party vendors and supply chains.

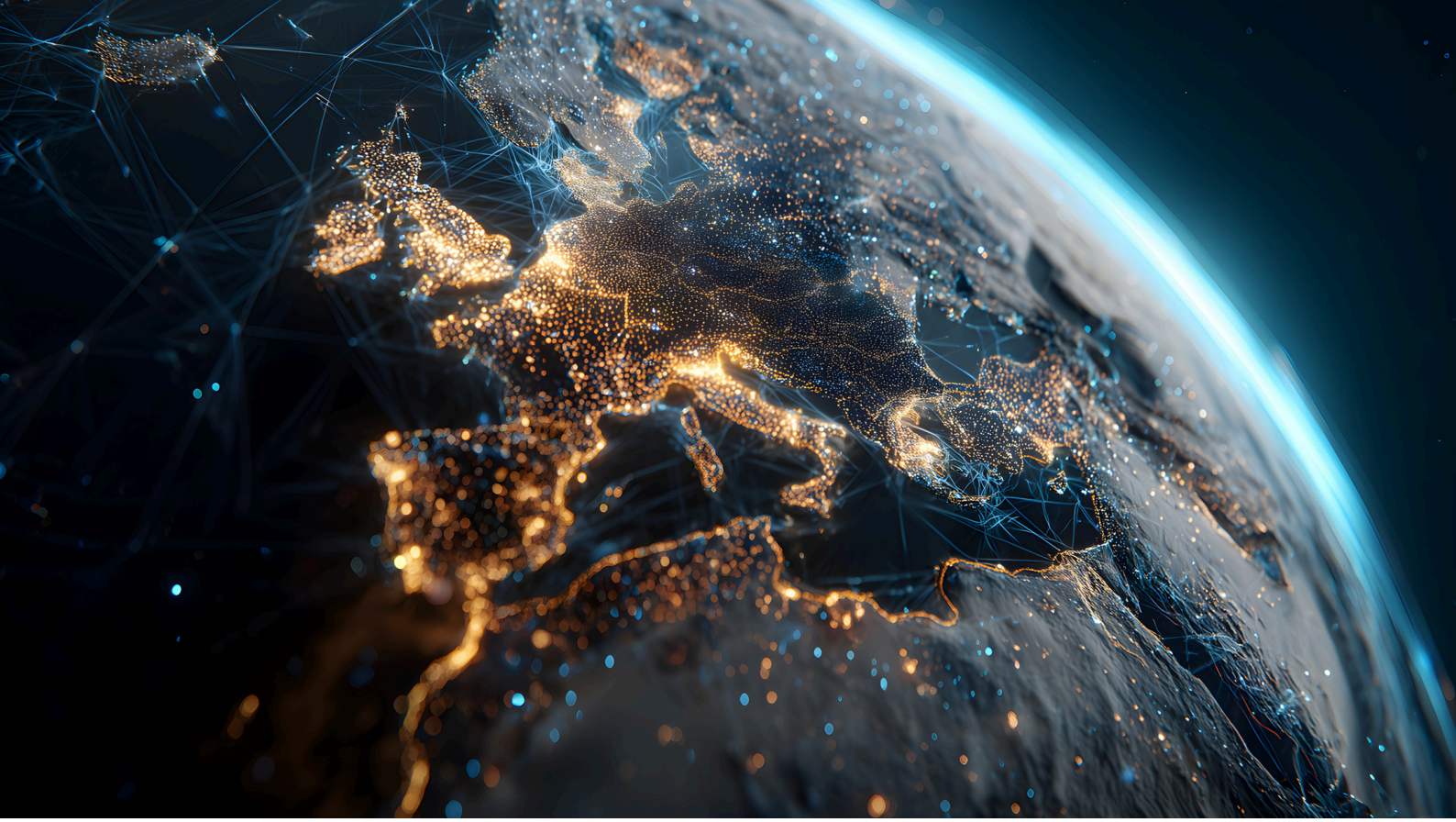
Malaysia's CSA mainly focuses on regulating NCII Entities and CSSPs. The 2024 amendments to the SG CA expanded its regulatory scope to include new categories like: Foundational Digital Infrastructure (FDI) providers (e.g., cloud services and data centres, even if they do not directly own a CII), Entities of Special Cybersecurity Interest (ESCI) and Systems of Temporary Cybersecurity Concerns (STCCs).

The SG CA's amendments also allow the Cyber Security Agency to regulate systems wholly located outside Singapore if the owner is in Singapore and the system provides an essential service to Singapore. The Singaporean amendment focuses on the location of the controlling entity (the owner/operator) and the impact of the service on Singapore. If a Singapore-based entity controls a system that is critical to Singapore's essential services, that system is covered, even if it is physically entirely offshore. Whereas the CSA's initial extraterritorial scope applies to NCII that is wholly or partly in Malaysia. In essence, the provision ensures that the law has the necessary power to protect Malaysia's vital national functions from cyber threats, regardless of where the attacker or the negligent party is situated, if the affected critical system has a link to the country's NCII entities. If a component or the operation itself is linked to Malaysia, it is covered.

In terms of similarities between the two Acts, owners and operators of the designated critical infrastructure must comply with similar core duties: conducting risk assessments and audits, adhering to Codes of Practice/Standards, and reporting cyber security incidents.



Both Acts establish a licensing regime for CSSPs to regulate the quality of services, especially those provided to critical sectors. Both laws have provisions for offences committed outside of their respective countries if those offences impact the nation's critical infrastructure.



DO MALAYSIA'S CYBER LAWS MEASURE UP TO EU STANDARDS?

Malaysia's CSA shares a strong resemblance with the European Union's primary cybersecurity regulation, the Network and Information Security Directive 2 (NIS2).

NIS2 is the EU's key framework for critical and important sectors; and significantly broadens the scope and imposes stricter requirements than the original NIS Directive. The similarities between Malaysia's CSA and the EU's NIS2 are in their sector focus and core requirements, which both mandate risk management strategies, incident reporting and breach notification procedures, clearly defined governance roles, regular security audits and vulnerability assessments, and resilience testing to ensure readiness against threats.

NIS2 is mandatory across the EU and brings higher expectations — and penalties — than before. Noncompliance can lead to significant fines and even personal liability for company leadership. The significant difference between the CSA and the NIS2, is the personal liability that company leadership face in case of noncompliance.

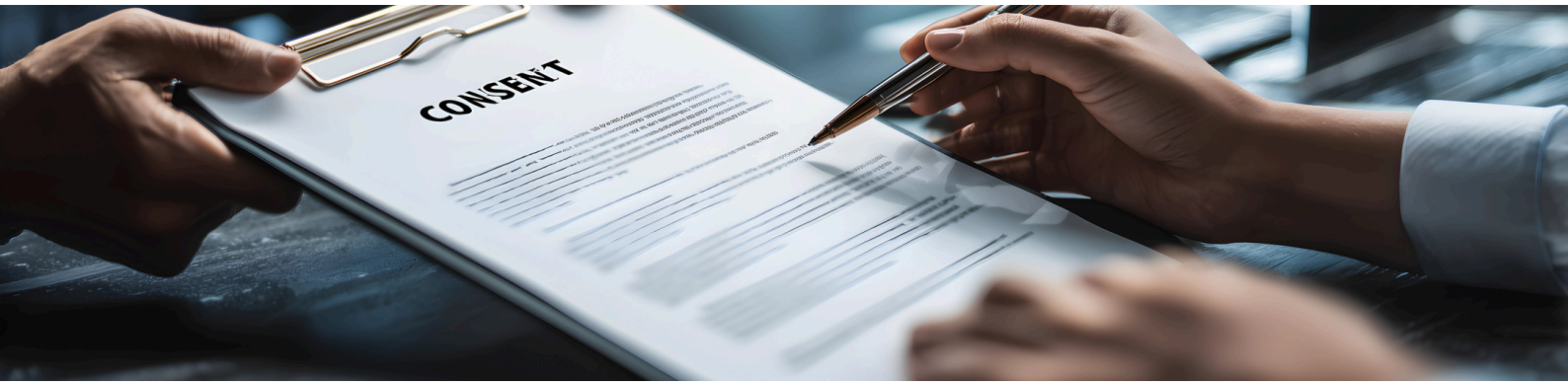
The GDPR is the EU's flagship regulation for data privacy and security. It has become the de facto global benchmark for privacy regulation, influencing new laws in countries across the world (including the recent amendments to Malaysia's PDPA). It sets the standard for how organisations must handle personal data, regardless of whether they are based in the EU or simply processing data from EU residents. The Malaysian government's 2024 amendments to the PDPA brings it closer to the standards of the GDPR, but key differences remain.

The scope of application of the GDPR is very broad and applies to personal data processing across all sectors, including commercial, non-commercial, social, and governmental activities (except where exempted). Whereas the Malaysian PDPA primarily applies to the processing of personal data in the context of "commercial transactions." The Federal and State Governments are largely exempt.

The GDPR applies to all organisations—regardless of size or sector—that collect or process personal data of individuals in the EU. This includes companies based outside the EU if they target or track EU users (e.g. via websites, apps, or services).

While the PDPA also has an “extraterritorial effect” it applies to entities established outside Malaysia only if they use equipment in Malaysia to process personal data and those that use data processors in Malaysia. The PDPA does not apply to the Malaysian Federal Government, the State Governments, or any personal data processed outside of Malaysia unless it is intended for further processing in the country.

The GDPR sets a high standard for consent – it must be "freely given, specific, informed, and unambiguous". Implied consent is considered insufficient. The PDPA only requires explicit consent for Sensitive Personal Data, but implied consent can be sufficient in some other cases.



Penalties for the GDPR can reach up to €20 million (RM97,798,000.00) or 4 per cent of the global annual turnover, whichever is higher. Beyond compliance, GDPR builds trust with customers and business partners through transparent data practices. Recent amendments (in 2024) have increased the maximum fine to RM1 million (approx. €200,000 to €250,000) and/or imprisonment. The key difference is that PDPA penalties are fixed monetary fines, not calculated as a percentage of a company's global annual turnover.

While the PDPA is a strong domestic law that is actively evolving to be more compatible with the GDPR, particularly in areas like breach notification, data portability, and requirements for the Data Processing Officer (DPO), its penalties and scope remain less comprehensive.

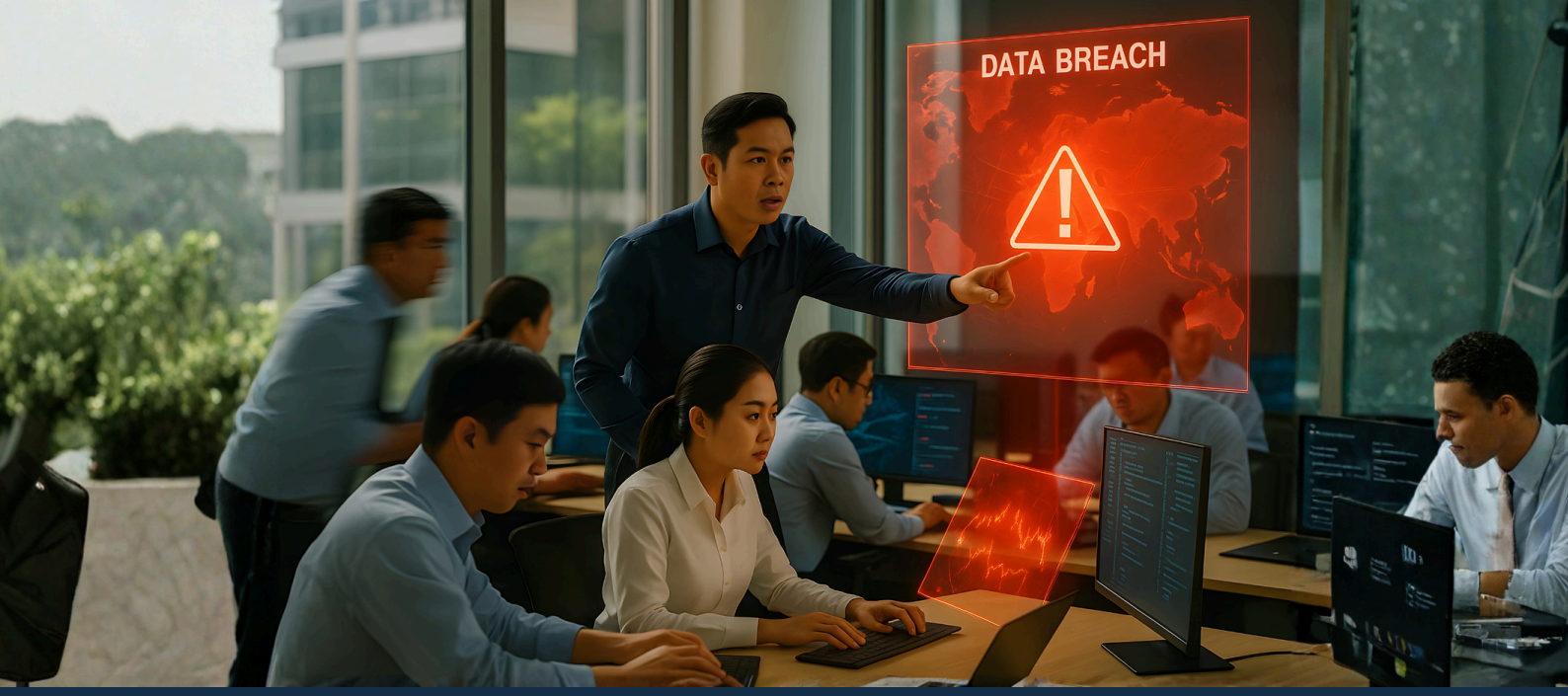
KEY CHALLENGES AND OPPORTUNITIES IN MALAYSIA

The CSA 2024 introduces significant changes that will have far-reaching implications for businesses operating in Malaysia, particularly those designated as NCII entities.

This could include increased costs, particularly in the areas of enhanced cybersecurity infrastructure, personnel, and potential penalties for noncompliance. This would involve upgrading existing systems, implementing new security protocols, and potentially hiring additional cybersecurity professionals. The requirement for regular risk assessments and audits will also incur ongoing costs.

Similarly, as Malaysia embarks on implementing data portability, the broad, non-sector-specific scope of these rights may challenge businesses across all industries, requiring them to develop secure processes and technologies, which could increase costs, especially for smaller enterprises.

On the flip side, the CSA also creates significant opportunities across the cybersecurity, technology, and professional services sectors with the explosion in demand for cybersecurity products and services across the 11 designated NCII sectors. It has created a high demand for qualified firms to conduct mandatory, periodic risk assessments, compliance audits, and gap analyses for hundreds of NCII entities, for purchasing and implementing security controls, software, and hardware to meet the new, stringent technical standards in the Codes of Practice. There will be an increased need for Managed Detection & Response (MDR) Services to ensure incidents are detected and reported to NACSA within the required short timelines. Finally, licensed providers gain a competitive edge and become the mandated choice for NCII entities seeking to outsource critical security functions.



CONCLUSION

Malaysia's CSA 2024 marks a significant step forward in strengthening the nation's digital defences through a more coordinated national effort and aims to create a more secure digital environment for both local and international companies operating in Malaysia. Future legislative changes may continue this trend, potentially broadening the scope to include areas like Virtual Critical Information Infrastructure (CII). It signifies the country's move from a largely voluntary and advisory approach to a mandatory, punitive, and focused regulatory framework for critical sectors.

However, businesses are still struggling with full execution, staff shortages, incident reporting hurdles, and disparate levels of preparedness. Feedback from early adopters (as reported in an article by Bank Info Security in September 2025) did raise questions about how much detail should go into six-hour incident reports, how severity thresholds should be defined and how to align overlapping obligations under the PDPA and CSA. Clearly, a considerable amount of work remains for businesses to grasp what compliance would mean in practice.

While recent laws provide a strong foundation, questions remain about Malaysia's readiness to address emerging technologies through legislation. The current legal framework still lacks specific laws for Artificial Intelligence (AI) and quantum technology.

For AI, only voluntary, non-binding National Guidelines on AI Governance and Ethics (AIGE) exist, and the Digital Minister has noted existing general laws are inadequate for AI-driven cybercrime. Similarly, the exponential growth of IoT in smart cities, agriculture, transportation, and energy expands the attack surface, necessitating secure device design standards, continuous monitoring, and anomaly detection frameworks. Proactive regulation and industry collaboration will enable Malaysia to harness technological innovation while preserving cybersecurity integrity.

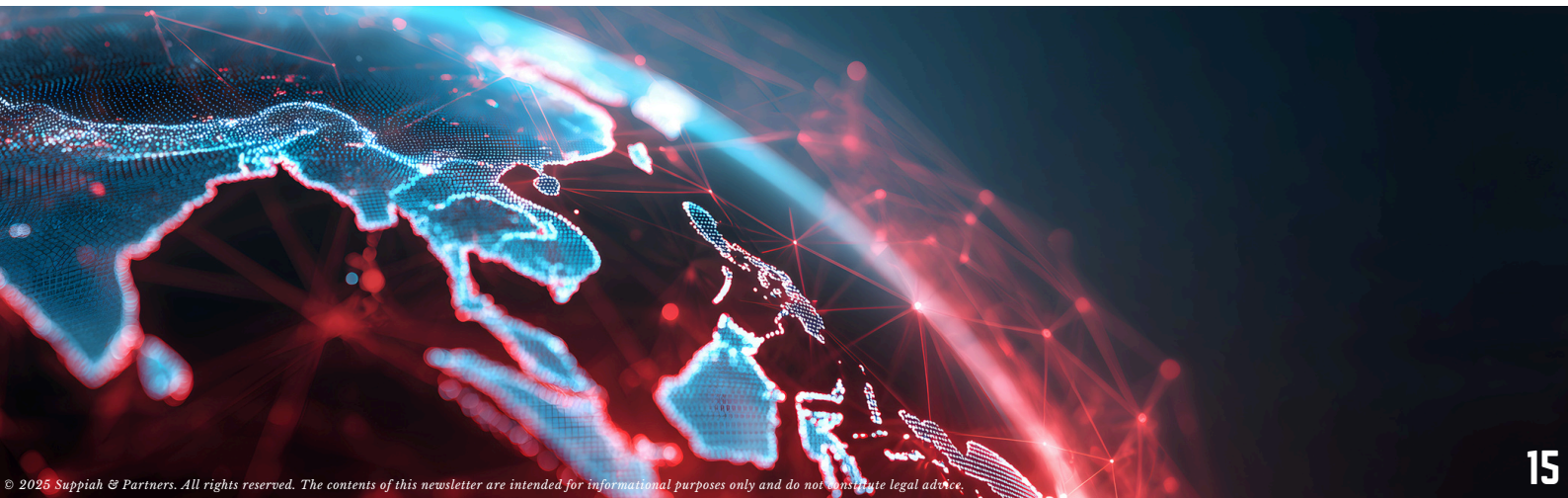
Meanwhile, specific, binding quantum cybersecurity laws remain under development. Although the CSA is a key step, the translation of domestic agreements into concrete, real-time mechanisms for cross-border cybersecurity collaboration and policy harmonisation is still a work in progress. Addressing these gaps will require targeted policies, added responsibilities to current agencies, or the creation of new departments.

RECOMMENDATIONS FOR STAKEHOLDERS AND POLICYMAKERS

To further strengthen Malaysia's cybersecurity posture, a concerted emphasis on public–private partnerships will be crucial. Such cooperation can foster information sharing, threat intelligence exchange, and coordinated incident response across sectors. Sector-specific cybersecurity forums, joint simulation exercises, and innovation incentive programmes can significantly enhance national cyber resilience. By cultivating trusted alliances that go beyond legislative mandates, Malaysia can better anticipate and mitigate the increasingly sophisticated threats confronting its digital economy.

Capacity building is also essential for Malaysia's cybersecurity ambitions. The persistent shortage of qualified professionals impedes effective implementation of CSA requirements across both public agencies and private enterprises. Expanding cybersecurity education and training, introducing targeted scholarships, and developing a robust ecosystem of certification and professional development programmes are necessary to address the talent gap and equip future leaders with expertise in emerging threat domains such as AI-driven attacks and quantum computing risks, to ensure the long-term sustainability of Malaysia's cyber defence capabilities.

As cyber threats are dynamic in nature, Malaysia's cybersecurity governance must remain adaptive and forward-looking. Ongoing regulatory evolution is essential to address fast-changing technological landscapes—particularly around AI governance, IoT proliferation, and cloud security. Establishing a regulatory sandbox, encouraging innovation-friendly policies, and implementing periodic legislative reviews will help balance stringent security measures with flexibility for digital growth. This will ensure Malaysia remains agile, resilient, and recognised as a trusted digital hub in Southeast Asia and beyond.



ADDITIONAL OUTLOOK FOR MALAYSIA'S REGULATORY FRAMEWORK – WHAT IS IN STORE

Just this month, Fintech News Malaysia, reported that to counter rising and increasingly sophisticated cybercrime, Malaysia is implementing a multi-pronged national strategy focused on structural and legal reform: at the core is the introduction of a comprehensive Cyber Crime Bill to replace outdated legislation, granting law enforcement the necessary legal strength to address complex digital crime and enhance national security. Furthermore, the NACSA is spearheading the creation of a new Centre for Cryptology and Cyber Security Development, which is envisioned as the national hub for advancing digital resilience and sophisticated cyber defences. Finally, to ensure a faster and more efficient response against scams, the National Scam Response Centre (NSRC) will be restructured under the Royal Malaysia Police (PDRM) to tighten coordination, accelerate incident handling, and streamline investigations.

Likewise, ongoing consultations on Data Protection Impact Assessments (DPIAs), Privacy-by-Design, and automated decision-making show that Malaysia is proactively addressing future technological challenges. These consultations are being led by the Personal Data Protection Department (PDPD) and are part of a broader effort to update the regulatory landscape following the Personal Data Protection (Amendment) Act 2024. By initiating public consultation on these advanced topics, Malaysia is effectively future-proofing its data protection laws to govern the ethical and secure use of emerging technologies.

REFERENCES

- Shaping the Digital Future: Regulatory Updates from Malaysia
- Malaysia Charts Its Digital Course: A Guide to the New Frameworks for Data Protection and AI Ethics
- Cyber Security Act 2024 (Act 854)
- Malaysia's Cyber Security Act 2024: Key Insights and Implications for Organizations
- Malaysia's Cyber Security Legal Landscape: Mandatory Compliance or Severe Penalties
- An Overview of Malaysia Cyber Security Act 2024
- Comparing EU cybersecurity frameworks: NIS2, GDPR, DORA and more
- Overview of Federal Laws Protecting Critical Infrastructure
- Malaysia Cybersecurity Job Market: Trends and Growth Areas for 2024
- One Year In, Malaysia's Cyber Law Is Showing Some Strain
- New Cyber Crime Bill and RM32 Million Boost to Tackle Scams in Malaysia
- Malaysia Cybersecurity Strategy
- Malaysia launches cybersecurity strategy amids growing threats
- 5 Pillars of Malaysia Cyber Security Strategy 2020-2024
- Malaysia's Personal Data Protection Department launches public consultations for data protection impact assessments, data protection by design, and automated decision making and profiling
- MOSTI sets framework for AI, quantum readiness

SUPPIAH & PARTNERS
since 2007

+603-4142 3766

https://suppiahlaw.com/

thulasy@suppiahlaw.com

UG-13, LEXA Galleria,
No. 45, Jln 34/26, Wangsa Maju,
53300 Kuala Lumpur

PREVIOUS NEWSLETTERS