CYBERSECURITY LANDSCAPE IN MALAYSIA 2025:

Navigating the Future Amidst the AI Revolution

As Malaysia embarks on its ambitious AI roadmap, developed by the Ministry of Digital Economy (MDE), it faces the critical task of fortifying its cybersecurity infrastructure. The increasing integration of artificial intelligence, IoT, and smart technologies into everyday life means that safeguarding the digital landscape is more important than ever. This article focuses on the current cybersecurity environment in Malaysia, the challenges ahead, and what more can be done to mitigate emerging risks in light of new digital advancements and increasingly sophisticated hackers. It was with this in mind that PIKOM created a PIKOM Cybersecurity Chapter, managed by an appointed team of experts and advisors five years ago.

1. Overview of Malaysia's Current Cybersecurity Landscape

Malaysia has made substantial strides in cybersecurity over the years. With the establishment of **CyberSecurity Malaysia (CSM),** a key government agency, the nation has strengthened its defences against cyberattacks, facilitated by national-level cybersecurity initiatives such as the National Cyber Security Policy (NCSP) and the Malaysia Cyber Security Strategy (MCSS).

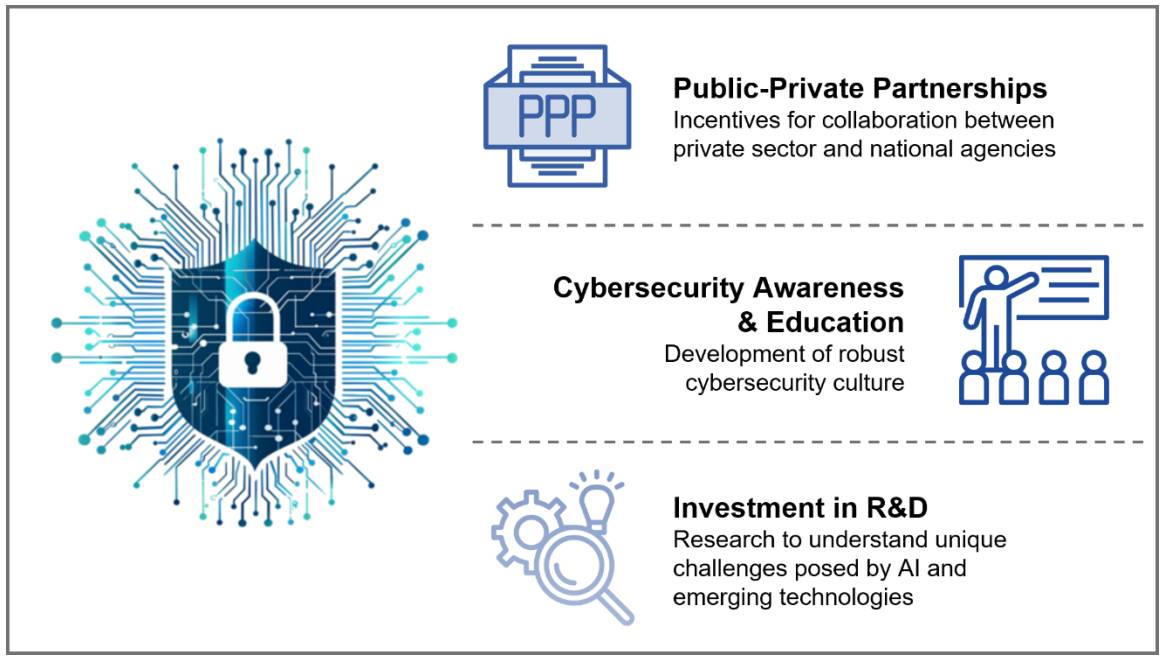
The revised Personal Data Protection Act (PDPA), which was amended in 2022, provides clearer data protection guidelines, ensuring that personal information is safeguarded in an increasingly interconnected world.

However, despite these efforts, challenges persist. Cybersecurity threats and breaches are growing in numbers and sophistication, from advanced persistent threats (APTs) to ransomware attacks. While Malaysia has witnessed improvements in its cybersecurity framework, we are still playing catch-up with the scale and pace of technological developments, especially with the rise of AI+, data, and cloud computing including several emerging and critical areas of concern for cybersecurity breaches today, such as IoT, 5G networks, supply chain vulnerabilities, remote work environments, quantum computing, and more.

Additionally, Malaysia's cybersecurity talent pool remains insufficient, and local enterprises, especially SMEs, struggle to keep up with the evolving threat landscape. With the evolution in the sophistication of the 'attacks', the skills and knowledge also need to keep pace. To a certain extent, our education systems may not be able to keep up with the pace and vigor of this rapid evolution and changes in skill set requirements.

2. What More Can Be Done Beyond Regulation?

Regulation alone may not be enough to fully secure the nation's cyberspace. In addition to tightening regulations such as the PDPA and creating a conducive framework for AI governance, several actions can be considered to further fortify Malaysia's cybersecurity posture:

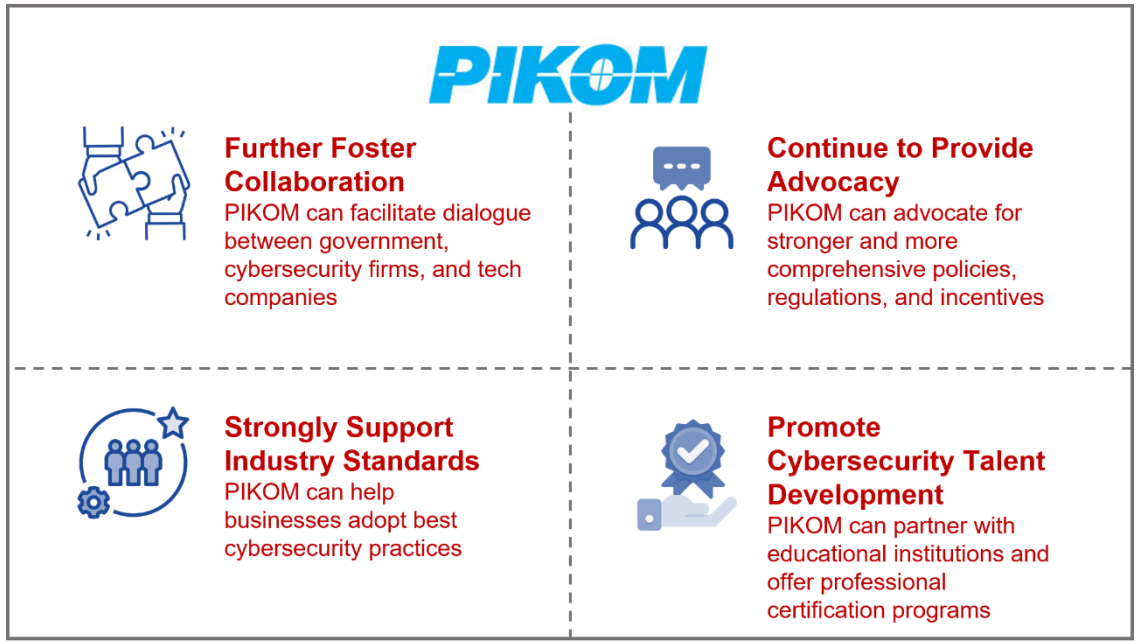


Public-Private Partnerships: The government should incentivize collaboration between the private sector and national agencies. Malaysia could benefit from greater engagement between tech companies, cybersecurity firms, and government bodies to build innovative solutions and risk mitigation tailored to the country's unique challenges.

- **Cybersecurity Awareness & Education:** Building a robust cybersecurity culture is essential. Cyber hygiene must be ingrained from a young age, and corporate and government employees should undergo regular training and inculcations. Public awareness campaigns and educational programs can ensure Malaysians understand the importance of digital security and practice safe online behaviours. Ethics and governance must be the cornerstones in this area. PIKOM Cybersecurity Chapter's annual Future of Cybersecurity Summit is one such event.
- **Investment in Research & Development:** Malaysia also needs to focus more on cybersecurity research to understand the unique challenges posed by AI and emerging technologies. Supporting local cybersecurity startups and facilitating innovation will enable Malaysia to develop homegrown solutions that can address specific threats to the region. We should not be just a community of tech adopters; cultivating a solution-creating mindset is equally critical to keep the balance.

3. What Role or Advocacy can PIKOM Play as an Industry Association?

As the national industry association (celebrating its 40th anniversary in 2026) for the IT and digital sector in Malaysia, PIKOM (The National ICT Association of Malaysia) has a crucial role to play in strengthening the nation's cybersecurity posture. Furthermore, with a Cybersecurity Chapter already in place for five years, PIKOM can:

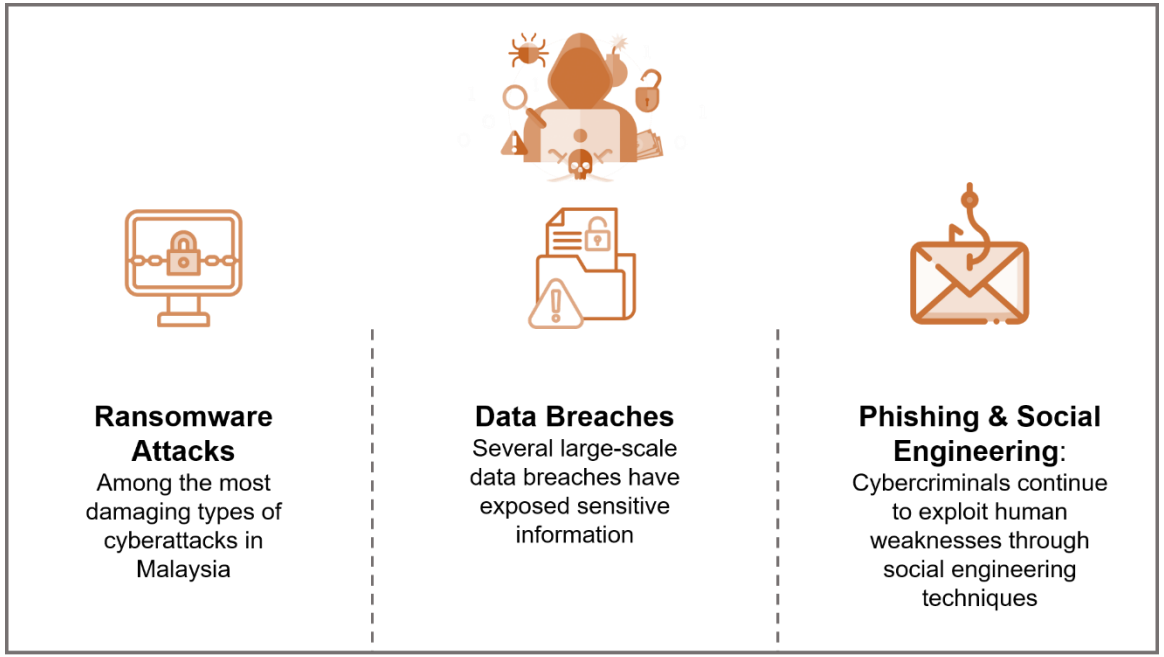


- **Further Foster Collaboration:** By bringing together stakeholders from the government, cybersecurity firms, and tech companies, PIKOM can facilitate important dialogue on the latest cybersecurity threats, trends, and solutions. This can also involve building partnerships with international cybersecurity associations to promote cross-border collaboration.
- **Continue to Provide Advocacy:** PIKOM can advocate for stronger and more comprehensive policies, regulations, and incentives to foster cybersecurity excellence within Malaysia. This includes pushing for **more investment in cybersecurity education** and highlighting the need for national-level coordination to address cyber threats.
- **Strongly Support Industry Standards:** PIKOM can play a pivotal role in helping businesses, particularly SMEs, adopt best cybersecurity practices. By developing industry guidelines and standards, PIKOM can make cybersecurity less daunting for businesses that lack in-house expertise. PIKOM can also engage the experts to conduct regular sessions on these industry Standards on the how, why and impact.

- **Continue to Promote Cybersecurity Talent Development:** PIKOM can partner with educational institutions and offer professional certification programs to address the cybersecurity skills gap. This would help ensure that Malaysia has a steady pipeline of skilled professionals to address the growing demand for cybersecurity expertise. Relevant TVET programs are perhaps one of them. PIKOM can also partner with their members to provide internships and programs specific to cybersecurity-related curriculum and in doing so provide on-the-job learning.

4. What Are the Latest Breaches in the Industry?

Despite the best efforts to secure systems, cyber breaches continue to be prevalent across industries. Recent high-profile attacks have included:



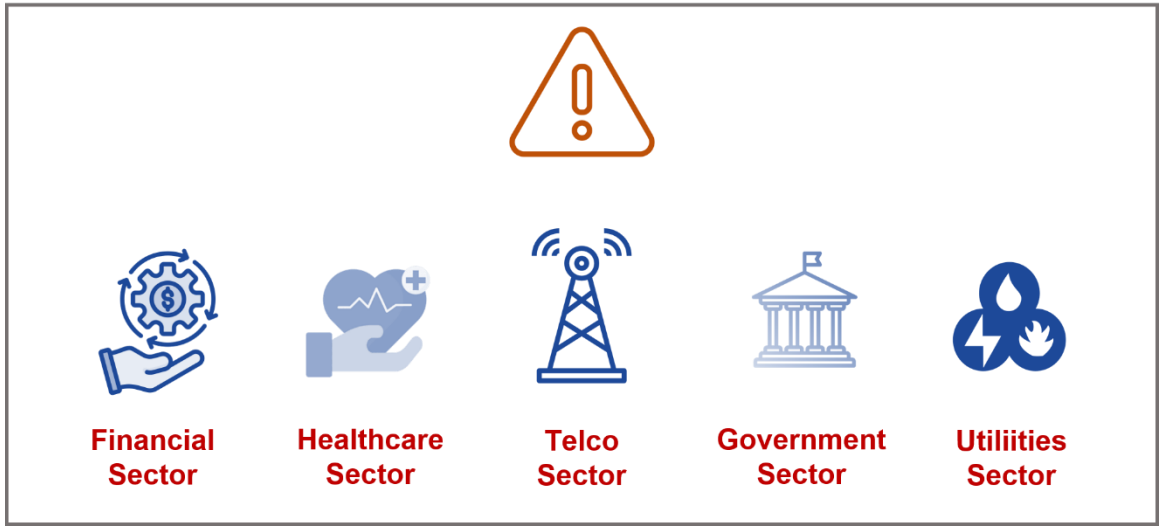
- **Ransomware Attacks:** These are among the most damaging types of cyberattacks in Malaysia, with businesses and even public institutions falling victim to ransomware operations. Cybercriminals demand payment in cryptocurrency for the decryption of stolen data, which results in both operational disruption and financial loss.

- **Data Breaches:** Several large-scale data breaches have exposed sensitive information. For example, major Malaysian telecom and banking institutions have had their systems breached, compromising customer data such as passwords and financial details.
- **Phishing & Social Engineering:** Cybercriminals continue to exploit human weaknesses through social engineering techniques, including **phishing and whaling**. Many individuals still fall victim to fake emails or calls, jeopardizing their personal and financial information.

These breaches underscore the vulnerability of Malaysia's cybersecurity framework and the urgent need for further comprehensive protection mechanisms.

5. Which Sectors Are Most Impacted?

Certain sectors are more vulnerable to cyberattacks than others, including:



- **Financial Sector:** With large volumes of sensitive data and financial transactions, banks and financial institutions are prime targets for cybercriminals. The risk of financial fraud and data theft remains high. The BNM RMIT paper has continuously emphasised the importance of these and made it onerous for management and directors.
- **Healthcare:** Hospitals and healthcare providers store vast amounts of personal health data, making them a target for ransomware attacks and data breaches.

- **Telecommunications:** As the backbone of digital connectivity, telecom companies are frequently targeted, with attackers seeking to exploit weaknesses in their networks to gain access to customer data.
- **Government:** Public sector institutions, especially those responsible for critical infrastructure, are also prime targets for cyberattacks aimed at disrupting national services or stealing confidential information.
- **Utility and Energy:** The energy and utilities sector is particularly vulnerable to cybersecurity attacks for several reasons - Critical Infrastructure, Aging Infrastructure, Increased Digitalization, Interdependency, high-value Targets, and prone to growing Threat of Nation-State Attacks. For example, the Colonial Pipeline attack in the U.S. led to widespread fuel shortages across the East Coast.

6. Scamming and Financial Losses: A Growing Concern

Scams are on the rise in Malaysia, with individuals (especially the older generations) losing significant amounts of money due to online fraud. Financial scams, investment frauds, and phishing attacks have led to millions in losses. People are often tricked into sharing their bank account details, clicking on malicious links, or falling for fake investment schemes.

In recent days, the role of **AI** and **machine learning** in scamming has become more pronounced. Cybercriminals use these technologies to craft highly sophisticated fraudulent schemes that are harder for individuals to identify. The government, in partnership with financial institutions and law enforcement, needs to increase efforts in educating the public about the dangers of online scams and providing more stringent consumer protection. Lately, we even heard that a person was impersonated in audio and video (using AI) on social media!

7. Are Current Laws Adequate?

While Malaysia has made significant progress with the Personal Data Protection Act (PDPA) and Computer Crimes Act 1997, the laws may not be fully equipped to handle the rapid pace of technological advancements. As cyber threats evolve and become more sophisticated, regulations must keep up. AI-based cybercrime and the potential use of quantum computing for malicious purposes are areas where current laws are silent or underdeveloped. The implementation of the Cybersecurity Bill, expected to be tabled soon, will be a critical step in updating Malaysia's legislative framework to address emerging threats.

Another key question is whether the penalties meted out to perpetrators are aligned with the seriousness of the breach? (a consideration that the lawmakers and legal profession need further consultations and deliberations)?

8. Who Can We Emulate from Other Economies?

When it comes to cybersecurity, Malaysia can draw inspiration from countries that have built robust digital defences, such as:

- **Estonia**: A leader in digital governance and cybersecurity, Estonia has set a global benchmark by creating a highly secure and interoperable e-government system. Estonia's X-Road digital infrastructure and emphasis on cybersecurity in public policy serve as excellent examples for Malaysia.
- **Singapore**: Known for its Cyber Security Agency of Singapore (CSA), Singapore has demonstrated proactive leadership in cybersecurity, focusing on national-level resilience and collaboration between government, businesses, and academia.
- **Israel**: Israel's highly advanced cybersecurity capabilities are globally acknowledged. The country's Israel National Cyber Directorate (INCD) focuses on protecting critical infrastructure, sharing intelligence, and preparing for cyber threats at the national level.

Conclusion

As Malaysia stands at the crossroads of digital transformation, the critical importance of cybersecurity cannot be overstated. The rapid pace of technological advancements—especially with the integration of artificial intelligence—presents not only unprecedented opportunities but also significant risks. The cybersecurity landscape is evolving, and to ensure that Malaysia thrives as a global digital economy, it is imperative that we take bold, collective action now.

The revised Personal Data Protection Act PDPA and the upcoming Cybersecurity Bill offer a solid foundation, but they are only part of the equation. Beyond regulatory frameworks, the true strength of our cybersecurity will come from a national effort - shared commitment among the government, private sector, and citizens to actively contribute to a safer digital environment.

PIKOM and industry leaders must take up the mantle of leadership in fostering collaboration, advocating for stronger cybersecurity practices, and ensuring that the talent pool is both adequately skilled and prepared for emerging threats.

The role of the business community, particularly SMEs, is pivotal; ensuring that they are equipped with the right tools, knowledge, and resources will be key to maintaining our national cybersecurity posture.

Ultimately, this isn't just about preventing cyberattacks – it's about safeguarding the trust that underpins our digital economy and protecting the data and privacy of millions of Malaysians, from individuals to enterprises. It's also about ensuring that the digital space remains a haven for innovation, allowing businesses to grow, new technologies to flourish, and Malaysians to embrace digital transformation without fear from domestic and foreign.

By drawing inspiration from global leaders, strengthening our policies, and creating a culture of cyber resilience, Malaysia can emerge as a beacon of digital security and trust in the region. But this requires unified effort—because cybersecurity isn't just an issue for IT specialists or regulators; it's a collective responsibility that every sector, organization, and individual must take seriously. Only then can Malaysia truly harness the potential of its digital future, with the confidence that its cyber borders are well-guarded.

This article is published by PIKOM Research Committee in collaboration with PIKOM Cybersecurity Chapter.

September 2025

E1, Empire Damansara, No 2, Jalan PJU 8/8A Damansara Perdana,
47820 Petaling Jaya, Selangor.
T +603-7622 0079 | E info@pikom.org.my I W http://www.pikom.org.my