

CYBERSECURITY & ASEAN: CLOSING THE GAP

WHY WE NEED A SINGLE, UNITED STRATEGY TO PROTECT OUR REGION ONLINE & ITS CORE CHALLENGES

Opinion

**VIKNESWARAN
KUNASEGARAN**
PROFESSIONAL FELLOW

Vikneswaran currently serves as Sr. Vice President at FIRMUS where he leads a team of consultants delivering security assessment services across Malaysia and the broader Southeast Asian region.



As digitization and e-commerce are on the rise, so are the threat actors and their ways of deceiving victims into cyber frauds. With an enhancement in the digital economy, it is of the utmost importance to ensure cybersecurity is also considered alongside to ensure it is sustainable. A total of US\$23.6 billion was the cost estimated for cyber incident victims across ASEAN in the year 2024 alone. The main reason for these cyber incidents are related to AI-driven deepfake attacks used for scams and financial frauds (Nur Ashkin Abdul Aziz, 2025). This data was taken from the Global Anti-Scam Alliance study, which is known for getting sample data across the world in relation to cyber scams.

This was mentioned by ASEAN Secretary-General Dr. Kao Kim Hourn during his speech at the 10th ASEAN Ministerial Conference on Cybersecurity (AMCC) held in Singapore last October 2025. This is considerably a large amount of money, especially in ASEAN, which

has only 10 countries (now 11, with Timor-Leste).

On 24th October 2025, the ASEAN Economic Community (AEC) Council announced the conclusion of the ASEAN Digital Economy Framework Agreement (DEFA) after 14 rounds of constructive negotiations to make this the world's first and most comprehensive regional agreement on the digital economy (ASEAN ECONOMIC COMMUNITY COUNCIL STATEMENT ON THE SUBSTANTIAL CONCLUSION OF THE ASEAN DEFA NEGOTIATIONS, 2025). With a total of US\$23.6 billion estimated for cyber incident victims across ASEAN in the year 2024 alone. The main reason for these cyber incidents is mainly related to AI-driven deepfake attacks used for scams and financial frauds (Nur Ashkin Abdul Aziz, 2025).

DEFA is trying to achieve seamless integration.

In Singapore, for example, despite being Malaysia's neighbour, there is zero difficulty when using the same application for travelling, ordering food, and even payment at stores. This scenario represents a microcosm affecting one individual who is travelling to another neighboring country. DEFA has the scope to achieve it on a macroeconomic scale across ASEAN. Developing this magnanimous framework means combining a seamless digital economy between 11 countries, coming with the responsibility of protecting it as well.

Dealing with a huge digital economy market, estimated to be around US\$2 trillion by 2030 (DIGITAL ECONOMY FRAMEWORK AGREEMENT (DEFA): ASEAN TO LEAP FORWARD ITS DIGITAL ECONOMY AND UNLOCK US\$2 TN BY 2030, 2023). It is inevitable that with the digital economy on the rise, so will cybersecurity. As mentioned earlier, cyber threats are everywhere, and rapidly rising day by day. New threats, new methods of scamming people, and new ways to abuse legitimate services/functions become the most apparent. With the AI accessibility, it's becoming even faster and even harder to detect. Although it was a step in the right direction to include cybersecurity as one of the critical pillars to support digital economy growth in DEFA, there are some key issues that have not been properly addressed.

The first would be the talent gap. According to the World Economic Forum, there is a shortage of 2.8 million to 4.8 million cybersecurity professionals all over the world (WEF GLOBAL CYBERSECURITY OUTLOOK, 2025). Almost 2/3 of the organizations worldwide are unintentionally left vulnerable to cyber threats, incidents, and breaches due to a lack of employees with the necessary skill set. This number is alarming: even in Malaysia, it is difficult to find a suitable cybersecurity talent with the right skillset to execute the job. Moving towards a mass digital economy does not translate to having a shortage of people to maintain and manage the security of those components. Framework then is strained as the security aspect is not sufficient to support its sustainability. The Privacy Framework is also another issue that needs to be recognized. In a digital age, privacy is everything. With hacks and breaches happening all around the world, personal data is something of interest to the threat actor to expose and monetize.

Having a big digital economy as such would require a stricter privacy framework to ensure all parties involved are held responsible for any mishaps in the future regarding data exposure. As Malaysia has also revamped the Personal Data Protection Act (PDPA), this can further be continued to be negotiated with other countries involved in finding a sweet spot for the privacy framework. An example of this is the EU General Data Protection Regulation (GDPR) is still one of the strongest data privacy policies in the world with a hefty fine structure! Maybe that can be used as a base, and the data privacy policies can be built on top of it.

Finally, arguably a companion, and chat buddy, Artificial Intelligence (AI). AI is at the forefront of technology currently; almost everything and anything now has an AI-enabled feature in it. With everything having AI, this ramps up the cyber threats. Though there are not many attacks seen using AI (because the traditional security flaws are still available for threat actors to abuse), it's on the rise. An interesting article from Anthropic, a US-based AI company that developed the large language model (LLM) named Claude, investigated the first reported AI-orchestrated cyber espionage campaign using agentic AI. Reported cases related to AI-based attacks, though, are on the low side with very minimal information on the news, but based on the severity of the issue, it is not something that can be ignored. There must be preparation for AI and what it may bring in the future. Malaysia has been in the forefront of this, where they are driving the new regional framework called ASEAN AI Safe Network, established in January 2025.

The main purpose of this is to accelerate regional economic growth (especially through DEFA), build safer digital environments by combating online scams and ensuring proper AI governance, among others. These measures aim to protect individuals and businesses from cyber threats while promoting trust and safety in digital spaces. This also extends to enhancing regional connectivity, as Malaysia, during ADGMIN, advocated for consistent digital and cybersecurity standards across ASEAN to ensure the interoperability of solutions. This benefits people by enabling seamless cross-border digital services, fostering innovation, and improving access to digital technologies across the region (Accelerating Regional Economic

Growth, Building Safer Digital Environment and Enhancing Regional Connectivity Key Takeaways for Malaysia at ADGMIN 2025 , 2025).

Integrating the digital economy across multiple countries is a good initiative but is only as strong as its weakest link. With different levels of cybersecurity maturity across the ASEAN nations, threat actors only have to find one vulnerability that could introduce a new attack vector which may impact other infrastructure. Integration cannot just stop by connecting systems, but it should be a collective effort to uplift the cybersecurity defence capabilities of the neighboring countries as well. Malaysia can spearhead a structured plan to bring developing nations up to speed by establishing policies and procedures in relation to cybersecurity, and most importantly building local talent to handle cybersecurity related matters.

In reality, cybersecurity must be seen as a value enabler rather than a cost center. Only if cybersecurity maturity is high, it enables countries to explore further on digitization and increase trust among the users to use the platform.

It is important to come up with a framework that helps to protect the platform from all three angles, which is people, process and technology. Only then can we ensure that ASEAN's digital rise is both rapid and resilient.

Malaysia can learn and develop artificial intelligence and eventually collaborate with the other ASEAN countries, where it will be a hub facilitating research and development work, safe and responsible development of AI, integrating AI across the public and private sectors, etc. This brings integration and interoperability of AI safety within the ASEAN countries.

Although Malaysia has been a great chair for the ASEAN 2025 Summit and excelled in producing results in DEFA and others, the US\$2 trillion digital economy targeted by DEFA is a huge project on its own. It requires a lot of work, talent, and technology to achieve the end goal or to even come near to it. In my opinion some of the key areas that Malaysia should focus on are mainly related to these two key areas.

References

Aziz, Nur Ashikin Abdul. "ASEAN Digital Economy Framework Agreement (DEFA) a Game Changer for Region: Experts."

Bernama, 24 Oct. 2025, asean.bernama.com/news.php?id=2481746.

"ASEAN Economic Community Council Statement on the Substantial Conclusion of the ASEAN DEFA Negotiations." ASEAN, 24 Oct. 2025, <https://asean.org/wp-content/uploads/2025/10/ADOPTED-AECC-Statement-on-Substantial-Conclusion-of-DEFA-Negotiations-24Oct2025.docx.pdf>

"Digital Economy Framework Agreement (DEFA): ASEAN to Leap Forward Its Digital Economy and Unlock US\$2 Tn by 2030." ASEAN, 8 Sept. 2023, <https://asean.org/asean-defa-study-projects-digital-economy-leap-to-us2tn-by-2030>

WEF Global Cybersecurity Outlook 2025. World Economic Forum, 2025,

https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf

"Accelerating Regional Economic Growth, Building Safer Digital Environment, and Enhancing Regional Connectivity: Key Takeaways for Malaysia at ADGMIN 2025." Digital.gov.my, 19 Nov. 2025, www.digital.gov.my/en-GB/siaran/ADGMIN-2025:Meningkatkan-Pertumbuhan-Ekonomi-Serantau-Membina-Lingkungan-Digital-Yang-Lebih-Selamat-dan-Meningkatkan-Keterhubungan-Serantau