Bolster nation's cyber defence system, say experts

KUALA LUMPUR: The country's cyber defence system must be strengthened to keep pace with rapidly evolving technology, particularly amid growing threats from radical extremist groups that use cyber attacks for generating income.

Universiti Teknologi Mara Media and Information Warfare Studies Centre security and political analyst Dr Noor Nirwandy Mat Noordin said while Malaysia's cyber defence system remains relevant, it must be reinforced, particularly in terms of speed and precision.

"Among the key strategies which can be used to enhance cyber security are strengthening capabilities in line with hackers' evolving modus operandi, and refining cyber emergency training, such as the National Drill, to ensure a high level of readiness."

Noor Nirwandy was referring to reports that Malaysia Airports Holdings Berhad's (MAHB) digital system had recently been targeted by hackers demanding a ransom of US$10 million (RM44 million).

Prime Minister Datuk Seri Anwar Ibrahim had said that the government did not bow to the threat.

He emphasised the need to bolster the country's cyber security by allocating additional funds to several agencies, including the police and Bank Negara Malaysia.

Noor Nirwandy highlighted the importance of international collaboration in developing a stronger and more resilient cyber security framework.

He said the National Cyber Security Agency (Nacsa) has been effective in monitoring cyber threats to the country.

Noor Nirwandy emphasised the need for greater collaboration between the government, private sector and the public to foster a cyber security-conscious culture and strengthen preparedness against evolving threats.

Universiti Putra Malaysia (UPM) Faculty of Computer Science and Information Technology cyber security expert Assoc Prof Dr Nur Izura Udzir said the cyber attack on MAHB's digital system also posed a risk to national stability.

"Cyber attacks of this nature can damage reputations, erode stakeholder trust, lead to operational losses and incur significant compensation costs. It is time for us to invest in national cybersecurity, particularly for critical infrastructure."

Nur Izura, who is also UPM Centre for Strategy and Corporate Relations deputy director (Strategic Management), and a member of Cyber Security Academia Malaysia, suggested exploring the use of artificial intelligence technology to further strengthen the nation's cyber security framework.

She also emphasised the importance of reducing Malaysia's dependence on foreign cyber security systems by advancing its own technological capabilities.

"Our country has many experts, including agencies like Nacsa, which can be further strengthened." – Bernama