Wake-up call for aviation security

THE cyber attack targeting Malaysia Airports Holdings Berhad (MAHB) along with a hefty US$10mil (RM44.4mil) ransom demand, which was revealed by Prime Minister Datuk Seri Anwar Ibrahim on March 25, is a stark reminder of the growing threats facing our aviation sector.

While the PM's decisive rejection of the ransom demand is commendable, the incident itself underscores a critical vulnerability – our skies, and the complex systems that manage them, are increasingly in the crosshairs of cybercriminals.

This isn't just a Malaysian problem; it's a global epidemic hitting the aviation industry. Japan Airlines was hit by a cyber attack in December 2024, disrupting flights and stranding passengers. On June 24, 2024, a cyber attack disrupted immigration and airport services, in Surabaya, Indonesia.

And who could forget the widespread IT outage linked to CrowdStrike earlier that same year? Though not malicious, it grounded thousands of flights worldwide, starkly highlighting our critical dependence on interconnected digital systems.

This vulnerability isn't new. Remember the massive data breach at Cathay Pacific back in 2018?

These aren't isolated incidents but clear warning signs of systemic vulnerability across the global aviation network.

As airports, airlines, and air navigation systems embrace digital transformation – cloud computing, IoT integration, artificial intelligence (AI) automation – their "attack surface" expands dramatically.

This makes them irresistible targets for everyone, from cybercrime syndicates seeking ransom to state-sponsored groups engaging in espionage, and even hacktivists looking to cause disruption.

The very technologies designed to improve efficiency are creating new avenues for attacks.

The numbers paint a concerning picture. Industry data suggests the travel sector is already one of the most targeted, facing a high volume of cyber attacks.

Experts predict this trend will only escalate in the coming years with more sophisticated ransomware and supply chain attacks on the horizon.

The PM is right to call for increased resources and technological sophistication for our relevant agencies, such as the police and Bank Negara, to enhance cybersecurity preparedness.

We simply cannot afford to be reactive, waiting for the next major breach or disruption to occur. We need sustained investment in building robust defences before disaster strikes.

This means adopting cutting-edge solutions. Experts recommend investing in AI-driven threat detection, implementing zero-trust security architectures (which assume no user or device is automatically trustworthy), leveraging real-time threat intelligence, and constantly adapting our security strategies to counter evolving tactics.

We must foster a culture of cybersecurity awareness across the entire aviation ecosystem.

Protecting our airports and airlines isn't just about preventing flight delays or financial losses; it's fundamentally about national security, economic stability, and passenger safety.

Digital threats are evolving at lightning speed; our defences must evolve even faster.

Let's ensure Malaysia is prepared for the turbulence ahead.

THULASY SUPPIAH
Kuala Lumpur

(The writer is a lawyer focusing on AI, data centres and cybersecurity.)