

# Cyber threats to aviation industry

The Star Malaysia · 6 Jan 2025 · THULASY SUPPIAH Kuala Lumpur (The writer is a lawyer focusing on artificial intelligence.)

THE recent cyberattack on Japan Airlines, while quickly resolved, serves as a stark reminder of the increasing vulnerability of the aviation sector. While the airline claims no passenger data was leaked, the disruption highlights a growing threat – our skies are no longer just vulnerable to weather patterns but also to digital storms.

The aviation industry is a prime target for cybercriminals. From ticketing systems to air traffic control, it relies on a complex web of interconnected IT systems. A successful attack can cripple operations, costing airlines millions in lost revenue and leaving passengers stranded.

But the financial fallout is just the tip of the iceberg. Data breaches can expose sensitive passenger information, and the potential for a cyberattack to compromise flight control systems is a chilling thought.

Imagine a hacker taking control of a plane mid-flight; it's a scenario straight out of a Hollywood thriller. But the threat is real. Cyberattacks are becoming increasingly sophisticated. Ransomware, DDOS attacks, and exploitation of third-party software vulnerabilities like the Crowdstrike outage in 2024 are just some of the tactics employed.

Remember that global IT meltdown that grounded planes, froze bank accounts and silenced news outlets? That's the interconnected world we live in, and aviation is right in the crosshairs.

The increasing use of AI and cloud technologies in aviation, while promising greater efficiency, also expands the attack surface. More connected systems mean more entry points for hackers.

And it's not just cybercriminals we need to worry about; nationstate actors and hacktivists also have the aviation industry in their sights.

In Malaysia, the Malaysian Aviation Commission (Mavcom) plays a key role in ensuring aviation security, working with other agencies and stakeholders to improve cybersecurity measures.

Cybersecurity Malaysia also plays a crucial role in effectively implementing national cybersecurity strategies and providing expertise to various sectors, including aviation. We need a robust, multilayered approach that combines strong regulations, cutting-edge security technologies and constant vigilance. We also need to invest in training and education to ensure that our aviation professionals are equipped to handle these evolving threats.

The question isn't whether another cyberattack will occur, but when. Let's hope we're ready when it does.