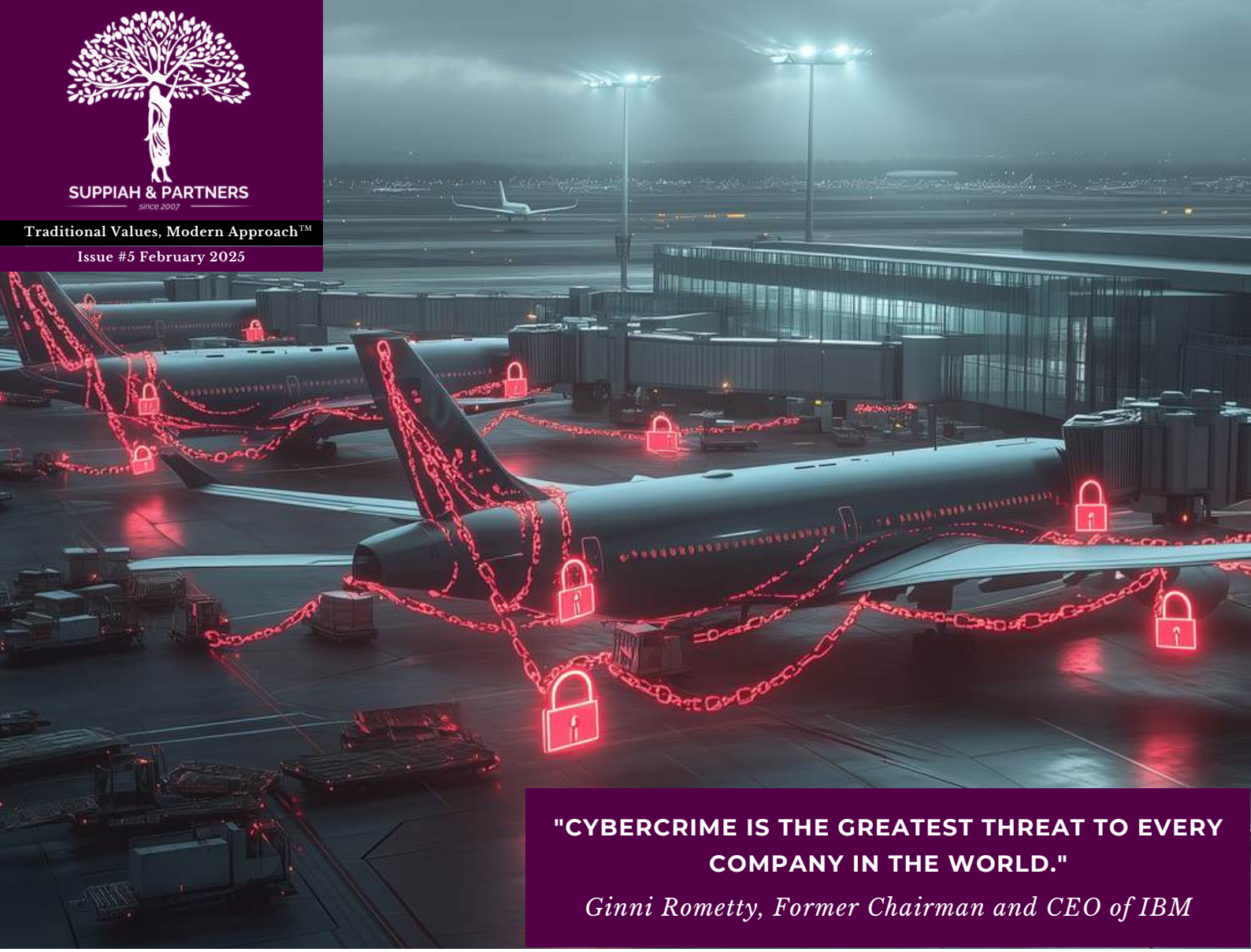
SUPPIAH & PARTNERS
since 2007
Traditional Values, Modern Approach™
Issue #5 February 2025



"CYBERCRIME IS THE GREATEST THREAT TO EVERY COMPANY IN THE WORLD."

Ginni Rometty, Former Chairman and CEO of IBM

GROUNDED BY CYBER THREATS

AVIATION'S GROWING DIGITAL VULNERABILITIES

by Thulasy Suppiah, Managing Partner

A few weeks ago, Japan Airlines (JAL) suffered a major cyberattack on one of the busiest days to fly – Boxing Day. While the resulting disruptions were temporary, it highlighted yet again the fragility of IT-dependent systems. Beginning 7.24 am local time, the attack targeted network equipment connecting internal and external systems. This led to both domestic and international flight delays, with the airline's app, and baggage handling systems also affected. At least 24 domestic flights were delayed by more than 30 minutes.

Whilst the threat was eliminated within a few hours, JAL had to temporarily shut down the affected router and suspended ticket sales for same-day flights resulting in considerable chaos and inconvenience to travelers. The airline later confirmed that the disruption resulted from a Distributed Denial of Service (DDOS) attack — their server was flooded with internet traffic to prevent users from accessing connected online services.

As airport, airline, air navigation and other travel or transport systems embrace digital transformation, including cloud migration, Internet of Things (IoT) integration, and AI-driven automation, its attack surface has expanded significantly. This makes the sector an attractive target for cybercriminals, nation-state actors and hacktivists.

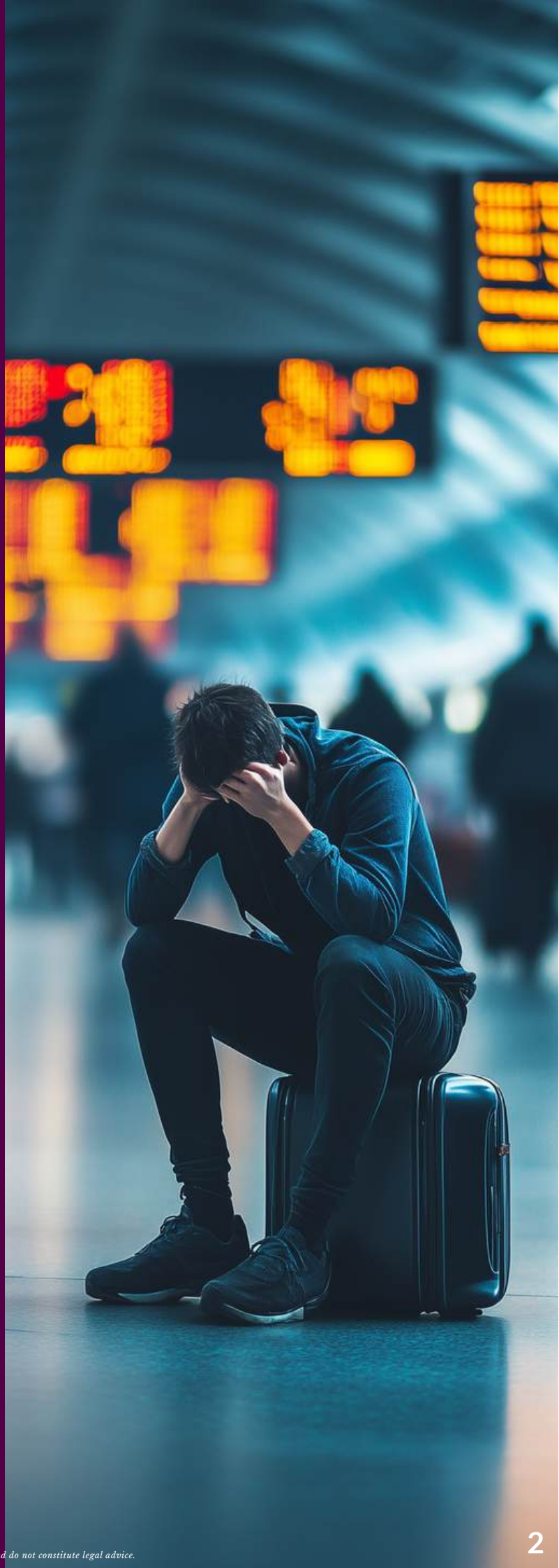
In July last year, an enormous IT outage linked to a faulty CrowdStrike update, disrupted airlines globally, grounding over 10,000 flights and highlighting the industry's reliance on interconnected digital systems. Though not a cyberattack, it had huge implications on airport systems and flights worldwide.

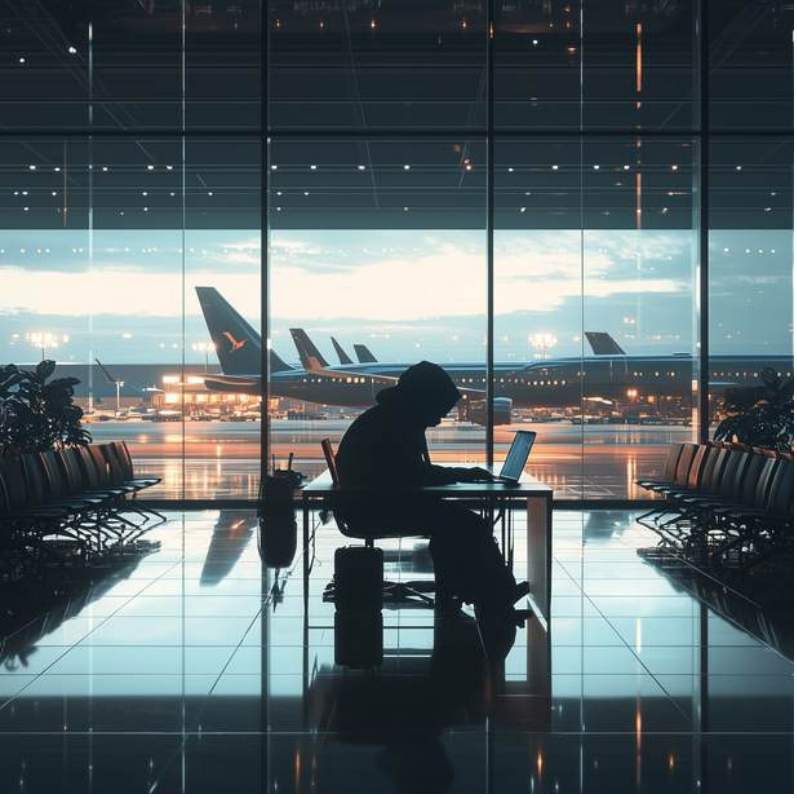
In June, Indonesia faced one of its worst cyberattacks with more than 40 government agencies impacted, and disrupting operations at major airports.

In 2018, Hong Kong's national flag carrier, Cathay Pacific Airways admitted to a data breach involving the extensive personal data of some 9.4 million customers. Passengers' personal information such as passport information including their nationality and date of birth; phone number; credit card information; identity card number; and even historical travel information was exposed.

In another ransomware attack last year, operations at Japan's largest and busiest terminal port in the city of Nagoya were paralysed – making it unable to load and unload containers for three days. Located just 7 km south of the terminal is Chubu International Airport, an air gateway that operates in coordination with the sea port. The attack on The Nagoya Port Unified Terminal System (NUTS) - such a critical infrastructure in Japan, handling 10 percent of the nation's trade - highpoints the significant ripple effects such incidents could have on essential services and supply chains not just in Japan but for the global economy.

Skift – an online source for travel news – highlighted an Imperva 2024 Bad Bot Report, which found that the travel industry suffered the second-highest volume of account takeover attempts in 2023. Around 11% of all cyberattacks targeted the sector and Cornelis Jan G, a Senior Cyber Threat and OSINT Analyst, from the Netherlands, says the aviation industry can expect to face an escalation in cyber threats in the next 12 to 24 months.





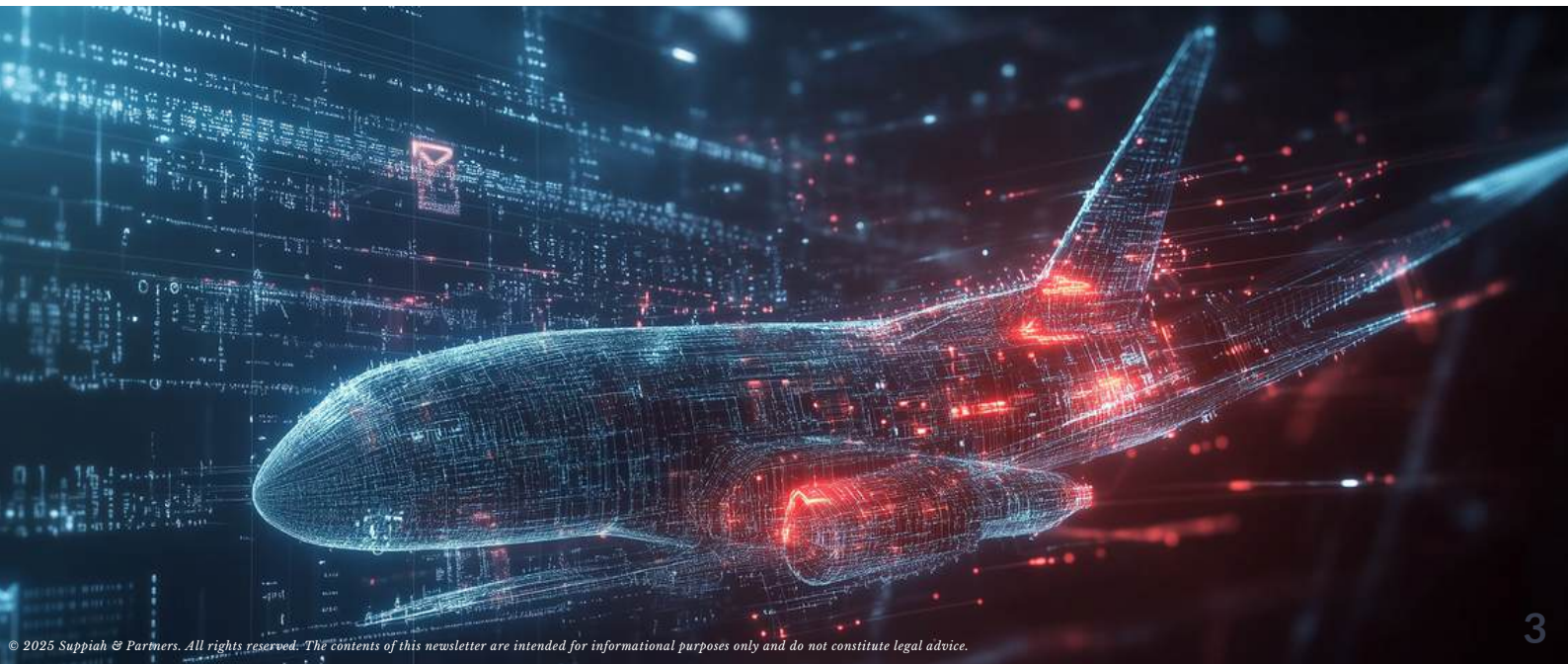
"State-sponsored groups will continue to target aviation for strategic intelligence and economic espionage, while cybercrime syndicates will increase their focus on ransomware and supply chain attacks," he wrote in an article (Reference Item 9). He believes the industry will benefit from increased investment in AI-driven threat detection technologies, and a focus on a zero-trust architecture which limits lateral movement within networks.

Callie Guenther, a cyber-threat research senior manager at Critical Start, in a comment to Infosecurity Magazine about the Nagoya cyberattack said, organisations need to stay informed about the latest ransomware trends, leverage threat intelligence sources to understand the evolving tactics, techniques, and procedures by ransomware operators, and adjust their security strategies accordingly.

For successful implementation of cyber security in the aviation industry, AI and tech-focused law firms play an imperative role. They provide essential and tailored legal services to navigate the complexities of AI integration.

Boeing for instance relies on its legal team to ensure compliance with strict Federal Aviation Administration (FAA) regulations and safety standards. United Airlines engages legal experts to establish guidelines for its AI applications in customer service, to prevent bias in AI algorithms and to ensure fair customer interactions. They also consult on transparency measures to let customers know how their data is used.Delta Airlines seeks risk management advice for AI predictive maintenance to mitigate potential liability issues related to operational failures.

Airbus engages legal services to negotiate contracts with its software vendors. These contracts are necessary to define the scope of work, data ownership and liability for AI-driven analytics. This is essential for the interests of both the aircraft company and the vendor, and to ensure compliance with aviation regulations.



REFERENCES

- Nagoya Port faces Disruption after Ransomware Attack
- National Cyber Security: Global IT outage not cyberattack, still caused considerable impact to Malaysia
- Major cyberattack disrupts holiday season flights at Japan Airlines
- Japan Airlines hit by cyberattack, ticket sales for flights departing on Dec. 26, 2024 suspended
- JAL's systems back to normal after cyberattack delayed flights
- JAL's system under cyberattack, domestic and int'l flights delayed
- Cyberattack hits Japan Airlines; flights delayed, ticket sales suspended
- Japan Airlines hit by cyberattack, delaying some flights
- Cyber Threat Intelligence Landscape and Actionable Forecast for Aviation Security Teams
- CrowdStrike outage explained: What caused it and what's next
- CrowdStrike: What the 2024 outage reveals about security
- The Cathay Pacific breach: a lesson in managing data protection risks
- Global standstill: could defensive AI have mitigated the impact on aviation and beyond?
- What is AI security?
- Leveraging AI as a Force Multiplier for Attack Surface Management
- Japan airlines under cyberattack, flights delayed
- Japan Airlines reports cyberattack on system, impacting flights
- Japan links hacker MirrorFace to dozens of cyberattacks targeting security, tech data
- Japan Airlines suffers major cyberattack; flights delayed, ticket sales halted

SUPPIAH & PARTNERS
since 2007

+603-4142 3766

https://suppiahlaw.com/

thulasy@suppiahlaw.com

UG-13, LEXA Galleria,
No. 45, Jln 34/26, Wangsa Maju,
53300 Kuala Lumpur

PREVIOUS NEWSLETTERS