Cyber Resilience in the Aviation Sector

‘Cyber’ is no longer an emerging risk. Network integrity and data security rank at the top of senior management concerns, as companies continue on the path to digitisation and interconnectivity.

The aviation sector has a distinct cyber risk profile, as companies have significant exposure to losses arising from data breaches as well as business interruption. Keeping air travel secure and efficient necessitates the collection of customers’ personal and payment information, making the industry a prime target for hackers. Computer systems also control critical functions throughout the industry supply chain, and reliable software is fundamental to essential operations, such as aircraft navigation, air traffic control systems, and passenger reservation and check-in. A minor system disruption can lead to severe global repercussions.

These developments have significantly increased the aviation industry’s exposure to cyber risks, extending beyond a data breach to encompass system disruption, property damage, and bodily injury. Therefore, it is imperative that aviation companies understand the potential for physical and financial damage arising from cyber attacks and focus on keeping systems secure.

Why Are Aviation Companies At Risk?

When considering exposure to cyber risk, aviation companies need to be cognisant of the danger presented by both targeted and widespread attacks.

Targeted Attacks

Targeted attacks are aimed specifically at an organisation. These attacks usually last for an extended period and typically involve more sophisticated malware. The threat posed to the aviation sector is amplified by the need to collect personal data from key clients.

Widespread Attacks

When vulnerabilities are identified in commonly used software, rather than in individual company systems, this facilitates a wide-ranging attack on any company using such programmes. The 2017 WannaCry and NotPetya incidents demonstrated the devastating impact and effectiveness of such attacks. Where companies in the aviation sector utilise the same processes, they leave themselves susceptible to coordinated, industry-wide attacks, or, once an individual company is successfully compromised, a series of copycat attacks exploiting the known vulnerability.

How a Cyber Event May Affect an Aviation Company

Hackers acquire the login credentials to loyalty programmes and issue fraudulent payments using customers’ rewards

Malware enters systems via a third-party vendor, spreading across networks, encrypting data and crippling communication, bringing operations to a standstill

A rogue employee accesses sensitive customers’ information. A data dump containing screenshots of account details is then published in the public domain

A hacker remotely gains access and compromises the avionics and other critical airplane systems, resulting in damage to the plane and injuries to passengers

We're here to empower results

To find out more about how Aon can help you address today’s cyber threats, please contact:

Gary Moran
+65 6239 7645
gary.moran@aon.com

Andrew Mahony
+65 6313 7080
andrew.mahony@aon.com

Sara Kobes
+65 6239 7627
sara.kobes@aon.com

AON
Empower Results®

What Damage Can Be Done?

The aviation industry is highly vulnerable to both data breaches and business interruption losses. Despite the evolution toward digitisation, the aviation industry traditionally allocates resources to physical rather than information and systems security. Aviation companies must realise that the consequences of not being prepared for a cyber incident can be severe.

Data Breach

The aviation sector has a large exposure to personal data which must be collected when passengers make flight reservations and payments. Numerous airlines have been the victims of large high-profile breaches, suffering significant losses when customer records are compromised. Hackers also target frequent flyer loyalty programmes, which are generally less securely managed than payment platforms, to make unauthorised purchases or offer the miles for sale on the dark web. Third-party companies entrusted to store data are similarly susceptible to the same risk.

Business Interruption

The aviation sector also has a significant exposure to business interruption losses, and companies must understand the repercussions that can arise when network security is compromised, or systems fail. Reputable airlines have experienced severe disruption to business operations, suffering considerable losses amounting to millions of dollars caused by seemingly minor disruptions. Such disruptions can result in persistent flight delays and cancellations for several days, with prolonged ramifications while companies work to get passengers and operations back on schedule. Whatever the cause, the damage has far-reaching and widespread implications, affecting the entire industry supply chain.

Organisations must prepare for contingencies in which a cyber attack causes physical damage. A number of identified exploits and attacks performed in the past decade have demonstrated that significant losses can be caused to physical assets when computer systems are compromised. This is an area of key concern for the aviation sector, particularly where sophisticated navigation systems are targeted, which can result in mass casualty and physical damage.

Given the vast number of customers the aviation industry serves on a daily basis and the responsibility for passenger safety, a cyber incident is likely to attract significant government and media attention. Regardless of the damage caused by a cyber incident, the company's reputation will be adversely affected, and it would likely be subject to substantial reparation costs, including expenditure on IT forensics and remediation, as well as public relations expenses where an attack occurs.

Past Attacks in the Aviation Sector

Business Interruption Due to System Failure

Southwest Airlines experienced a system outage in July 2016 when a single router at its data centre failed, crippling software applications. Although the outage was fixed about 12 hours later, the scale of the disruption wreaked havoc on Southwest's operations for several days as the airline worked to get planes, crew and passengers back to normal. In total, the airline reportedly cancelled about 2,300 flights in five days. Experts estimated the loss at USD54 million, possibly reaching USD82 million due to lost revenue and increased costs.

Frequent Flyer Miles Targeted

Lufthansa was the victim of a cyber attack in 2015 when hackers used a botnet to decipher customer login credentials used to access the airline's online portal. Once the correct combination of username and password was achieved, the hackers made purchases using miles accumulated on users' frequent flyer accounts. Hackers used miles to obtain vouchers and redeem rewards, mainly purchasing items that did not need to be delivered by mail.

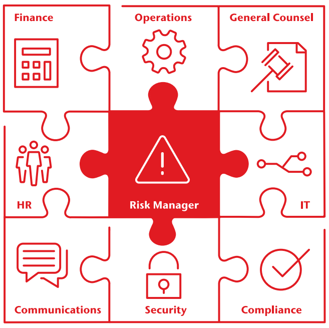
Data Breach

British Airways (BA) was hit by a data breach in September 2018, during which, more than 380,000 customers who had booked flights with the airline via its website and app during a two-week period had their personal and payment information stolen by hackers. BA promised to compensate any direct financial loss suffered by customers as a result of the breach alongside providing a 12-month credit rating monitoring service. Additionally, BA was threatened with a USD650 million class-action lawsuit that pointed to compensation rights in the General Data Protection Regulation (GDPR).

Distributed Denial of Service (DDoS) Attack

LOT Polish Airlines suffered a massive DDoS attack in 2015 that caused the airline's computers to crash and crippled its flight plan IT system. The airline was unable to carry out normal functions, resulting in a five hour disruption that saw 10 flight cancellations, 12 flight delays, and 1,400 passengers grounded. Thankfully, the attack only disrupted flights on the ground, and did not affect flights in midair.

What Can a Risk Manager Do?



- Work with your broker to understand how your existing policies respond to cyber events and how a cyber insurance policy can cover gaps
- Discuss with your IT, security, and operational colleagues what cyber threats keep them up at night and what protections are in place
- Prepare a Risk Register which identifies key cyber exposures and their potential impact to the business
- Look into a cyber insurance solution which provides affirmative property damage coverage

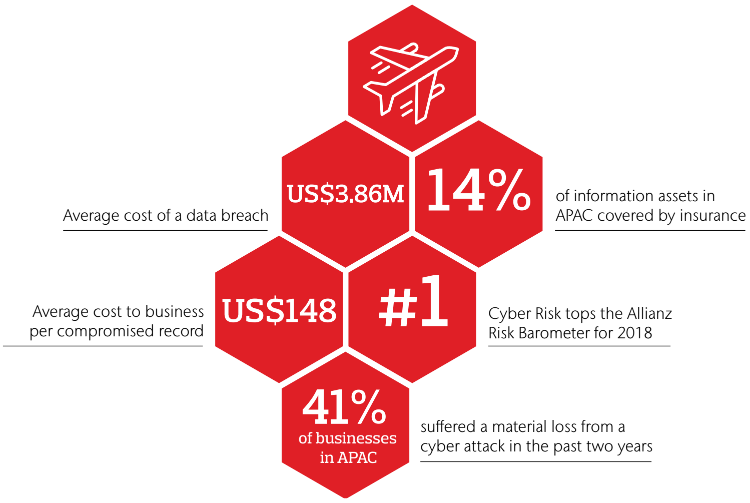
Improving Cyber Resilience

Recent cyber attack trends suggest that hackers are favouring a return to more rudimentary attacks in response to improving security measures, with spear-phishing and social engineering commonly employed. These attacks target human vulnerability primarily, so organisations must ensure adequate training and awareness are in place.

In order to assess the readiness of both systems and staff, it is recommended that senior leadership look outside the organisation for an objective audit of security. For example, “Red Team” testing of systems, being the engagement of ethical hackers to attempt to breach network security, is considered the gold standard of system testing, and allows senior leadership to assess, test, and understand how to improve cyber resilience.

By combining technical excellence with consulting and broking expertise, Aon is unmatched internationally in our ability to offer end-to-end cyber solutions for our clients, including proactive system testing, financial impact analysis, and managing cyber events.

Key Figures:



US$3.86M — Average cost of a data breach

14% — of information assets in APAC covered by insurance

US$148 — Average cost to business per compromised record

#1 — Cyber Risk tops the Allianz Risk Barometer for 2018

41% of businesses in APAC — suffered a material loss from a cyber attack in the past two years

How Can Aon Help?

Sophisticated entities recognise that risk mitigation and risk transfer are not mutually exclusive, but complementary.

The first step is to understand what exposures are currently uninsured, and how significant they might be. This requires a systematic and thorough assessment of existing policy response to cyber threats. In the aviation sector, traditional policies which respond to physical damage to tangible property are unlikely to respond to cyber attacks which target intangible property, such as data.

Our team can provide guidance as to how your current policy responds to cyber incidents and what solutions are available. These include cyber solutions which cover property damage, as well as providing broad coverage in respect of first party losses and third party liabilities that arise from data and network security breaches, including ransomware attacks, and cover lost income arising from system disruption events.

The Aon Cyber Solutions Group provides clients with holistic, enterprise-wide solutions that improve cyber resilience and support incident response. Our professionals are leaders in proactive services and digital forensics, who can deliver best-in-class testing that helps organisations identify and understand their vulnerabilities in order to effectively mitigate cyber risk.

Disclaimer: This risk and insurance description is a general summary for information purposes only. This does not purport to be insurance, legal or professional advice. For further advice on this or related insurance needs, please contact a representative of Aon.

Empower Results®