Navigating Aviation Cyber Risk

Published 24 March 2022

The civil aviation industry has experienced some of the most high profile cyber-attacks of recent years. In 2018, three huge breaches targeted major airlines; whilst British Airways and Air Canada lost control of a combined total of around 600,000 customer and staff records, Cathay Pacific suffered an attack affecting a whopping 9.4 million passenger records.

Whilst these vast data breaches have attracted a lot of headlines and column inches, regulatory enforcement action, and colossal reputational damage, they are not all that different, conceptually, from the ransomware attacks that we see every day as cyber-breach response counsel, targeting organisations from all sectors. So, much as we posed this question in reference to marine cyber in last month's DACB, what makes aviation special? Why is the aviation sector different, and why is specialist aviation cyber-insurance important?

Firstly, aviation has its own legislative and regulatory environment, so a cyber-attack on an airline or airport, for example, will generate its own set of discreet legal obligations in addition to those in place for other sectors.

The aviation sector is considered a part of the UK's critical national infrastructure ("**CNI**") and a number of aviation services are deemed to be essential. As a result, aviation falls within the auspices of the Network and Information Systems ("**NIS**") Regulations 2018, which were implemented to address the threat to security of network and information systems for those services deemed crucial to the operation of the state. Both the Civil Aviation Authority ("**CAA**") and the Department for Transport ("**DfT**") act as co-competent authorities for the NIS Regulations, with DfT being responsible for NIS policy and enforcement. DfT also sets the threshold for notification of NIS reportable incidents, which is separate and distinct from the UK GDPR thresholds maintained and upheld by the Information Commissioner's Office ("**ICO**").

In addition to the NIS Regulation, an array of aviation safety regulations apply to the sector's cyber environment. With digitisation embraced to a high degree in comparison with other industries, the potential cyber-impacts on operational safety are huge. The European Union Aviation Safety Agency ("**EASA**") Basic Regulation ceased to apply in the UK when it left the EU and ceased to be a member of the EASA community; however, all EASA requirements current on the withdrawal date (31 January 2020) have been retained in domestic legislation, including those aspects related to cyber-security for Aerodromes, Aeronautical Information and Air Navigation Service Providers.

In terms of security, as opposed to safety, regulation, the DfT has adopted an amendment to the Single Consolidated Direction 1/2021 which adopts certain cyber-security requirements for aviation into domestic law. These requirements relate to those elements of the aviation sector which fall within the National Aviation Security Programme, managed and regulated by the CAA.

All of the above is encapsulated within Civil Aviation Publication (CAP) 1753, the CAA Cyber Security Oversight Process for Aviation. This is a great reference point for anyone seeking to better understand the regulatory framework applicable to aviation cyber in the UK, and also includes significant insight on industry best practice and risk management/assessment.

In terms of risk, digitisation and networked operational technology has already been alluded to, but it is worth emphasising precisely what this means. Again, similarly to the marine sector, speculative stories about threat actors hacking automated systems to remotely control or sabotage aircraft attract headlines, but that risk is not particularly well supported by evidence. What is clear though is that any cyber-threat which undermines redundancy in systems, such as impairing safety monitoring or engine management systems could have a severe causational impact on flight safety. Equally, cyber-incidents impacting aircraft maintenance facilities may lead to delay, a failure to meet contractual obligations, and associated financial and reputational consequences.

Finally, as mentioned in the introduction above, the aviation industry is just as susceptible as any other for the theft and ransom of data that its organisations control. The difference is that the aviation sector is inherently international, the largest airlines have a truly global footprint and need to navigate a multi-jurisdictional regulatory environment that can seem perilously complex without the support of appropriately experienced local legal expertise. Furthermore, the very nature of the data held by airlines and airports is inherently attractive; consider the degree of personal detail that you submit in order to book an international flight, and it is very easy to imagine the value that such data holds for a person seeking to take advantage of your finances, identity, or lifestyle.

DAC Beachcroft's established Aviation and Cyber and Data Risk teams are coming together, combining their deep respective expertise to provide aviation cyber-breach response and advisory services. If you would like to discuss how DAC Beachcroft can assist both insurers and insureds across the aviation sector, please do not hesitate to contact Alex Stovold or Tom Evans using the details below.

Authors

Alex Stovold
London - Walbrook
+44(0)20 7894 6251
astovold@dacbeachcroft.com

Tom Evans
London - Walbrook
+44 (0)20 7894 6480
tomevans@dacbeachcroft.com

DAC BEACHCROFT