PIIQ PERSPECTIVE

Cyber insurance and aviation

Volume 11 June 2021

Whilst the pandemic continued to ground operations and drive the aerospace sector to a halt, despite the relative inactivity of airlines and manufacturers the increasing frequency of malevolent cyber-attacks, data breaches, ransomware and all out-system failures have continued to disrupt the sector. For the insurance market, evaluating and underwriting cyber risk presents a serious challenge, particularly given the last few years of wafer-thin underwriting profits. Consistent losses are driving profound changes in appetite for aerospace cyber risk and any airline considering transferring their risk into the insurance market should expect a high level of scrutiny.

Source: Bitdefender Report 2020

Aviation has continued to be a focus area for attacks and system failures with a 485% increase in ransomware attacks alone in 2020

Cyber and the fallout from an increasing number of incidents is now widely publicised and coupled with costly regulatory fines it is difficult to ignore. Just last week American Airlines experienced a sophisticated cyber-attack on their supply chain, leaving many aircraft without fuel (*Reuters, May 2021*).

In the UK, British Airways has been fined a record £20m for its 2018 loss of passenger data under GDPR legislation affecting some 400,000 staff and passengers (*Financial Times, October 2020*).

Cathy Pacific came undone by a cyber-attack that leaked the passport details of some 9.4million individuals worldwide (*Financial Times, November 2018*).

Despite best efforts, aviation has continued to be a focus area for attacks and system failures with a 485% increase in ransomware attacks alone in 2020 from 2019 (*Bitdefender Report 2020*).

THE INSURANCE MARKET AND CYBER RISK

The cyber insurance market has been rapidly expanding over the last few years, from $7.8bn in 2020 to $9.5bn in 2021 (*Fintech Times 2021*) and yet solutions for airlines have been comparatively slow to materialise. Aviation's strong focus on data and inter-connectivity has not been matched by fit for purpose cyber insurance solutions. Indeed, many brokers have been quick to roll out "off the shelf" policies or to simply transfer the same policy from another industry into aviation. The potential negative consequences of over-reliance on 'off the shelf' insurance products being used to meet the needs of unique risk profiles are obvious.

Part of the problem is insurer experience in aviation and cyber. The circumstances above have unsurprisingly contributed to a hardening of the market with rate increases, line size reductions and more stringent exclusions (in particular with a focus on limiting cyber extortion losses prevalent at the start of 2021). It is concerning that at a time when clients need innovation, they were being provided with inflexible solutions to coverage from some corners of the market.

Take for example a recent consultation one of our sister companies Ed Broking LLP had with an airline client. The airline in question had a forward-thinking view to cyber risk and had invested heavily in in-house resources to combat first party loss. This was an aspect of risk that the client did not want transferred and yet insurers were determined to offer the same off the shelf product regardless of suitability for the client. All hypothetical options thus far provided to the risk manager have included coverage for standardised first party costs, occasionally with certain enhancements bolted on. The enhancements may give the guise of a solution being 'tailored', but this is not tailored to their actual needs.

This is why in today's market it is incredibly important to find a partner that will truly take the time to listen and understand a business's concerns. A successful outcome requires a careful consideration of a business to allow underwriters to better evaluate, understand, and price risk. Preparedness is key, especially in a time when insurers are undertaking a forensic focus on underwriting information both at inception and renewal with specific focus on key risks such as ransomware. With the right strategy it is possible to achieve a good outcome.

The need to approach cyber insurance in the airline space with fresh eyes is glaringly obvious, and it is down to those arranging cover to take note of the growing need for sophistication within the service provided to clients.

LOOKING TO THE FUTURE

The insurance industry has a proven track record of adapting to changing risk environments. Aviation will be no different especially as improvements in cyber defence and processes make the sector a more attractive proposition.

Underwriters will need to focus on how to make policies relevant and applicable to the customer. Manufacturers and OEMs for example present an entirely different risk profile than an airline. From recent conversations Ed Broking LLP has had with a leading engine manufacturer it is clear that not being a passenger carrying entity means issues such as data breach are much less of a priority versus the risk of IP or design exposure. In the current market the sad truth is that both airlines and manufacturers may very well be offered the

same policy and it is clear how this approach is not applicable or relevant.

All of this points towards a market that needs to communicate better and deliver more relevant product for its customers. It is a misconception that customers do not know what they want. Whilst there is always room for education most in the aviation industry can see the need for a robust cyber contingency plan. This is reflected from increased scrutiny at the boardroom level with a particular focus on catastrophic loss triggered by a cyber event, with active concerns centred around availability of the insurance market capacity to absorb hundreds of millions of dollars of losses.

Looking to the future the market needs to evolve to meet specific needs and be relevant. In the long term that means designing "fit for purpose" policies that accurately reflect consumer demands. In the short term, creativity around programme design with retentions, sub-limits and line size is desperately needed. If applied correctly it is very likely insurers will find there are no bad deals, just bad structures, and bad prices.

FINAL THOUGHTS

In its current lifecycle the cyber insurance market is hardening in response to losses and a negative perception of the aviation industry in general. Scrutiny is being applied with laser focus to underwriting submittals and renewals are receiving more attention than in the past. Against this backdrop it is essential that the actual requirements of the client are identified before solutions are sourced. Only by following this order, can one ensure that the product built for any client meets their needs efficiently.

To do otherwise would be to waste budget on purchasing millions in limit on areas of coverage that is in fact redundant.

In the cyber market we see the most complex and intricate risk profiles from diverse industries around the world, and our solutions now need to be more malleable if they are going to work in conjunction with the unique risks that each industry faces. Last month's ransomware attack on the gas pipeline in the south-eastern United States is a pointed reminder that substantial risk to a company might not arrive via a direct cyber-attack that causes first party loss, but rather via contingent exposure to an attack to their supply chain in an adjacent industry.

Insurers and brokers must play their part to help their clients navigate these circumstances with real customisation in the way in which capacity is made available to the sector. It will be a poor reflection on our industry if product is not improved by more competitive markets, who are willing to demonstrate a pro-active and flexible approach to the risks they are underwriting.

AUTHORS

JOHN HEAD

Cyber team, Ed Broking LLP

John joined the cyber practice at Ed Broking during the summer of 2020, to help continue the impressive growth that the team has enjoyed during its first 4 years. John works with clients at all intersections of the insurance cycle within both the production and placement of business. Prior to joining Ed Broking John worked at the professional lines wholesale specialist Paragon International Insurance Brokers, where he worked within the cyber team helping provide bespoke solutions to clients ranging from SMEs to some of the largest cyber insurance structures placed globally.

Before his time at Paragon International Insurance Brokers, John gained three years of experience in the sector on the underwriting side. He worked at QIC Global writing Financial Institutions business as well as Cyber Treaty insurance for MGAs/Consortiums.

E: john.head@edbroking.com

M: +44 (0)7999 047103

BILL PARNELL

Senior Partner, Piiq Risk Partners Limited

Bill brings over 20 years of valuable experience working for two of the largest broking houses in the industry. Over the course of his career Bill has worked with a diverse group of global clients across all sub-sectors of aviation. He is committed to providing exceptional client advocacy and bespoke risk and insurance solutions.

Bill has held a variety of senior roles in the aviation insurance industry, most recently he was Placement Leader for the Aviation Practice at Marsh. Thus, Bill also has an interest in placement activities and helping design mechanisms that empower colleagues to deliver value for clients both now and in the future.

E: bill.parnell@piiqrp.com

T: +33 (0)20 8148 3693

M: +44 (0)7513 135900