Cyberinsurance takes specific flight path for airlines

by Jamie Monck-Mason

When discussing cyber attacks stemming from the *Internet of Things,* few scenarios strike more fear into the public than that of an airliner brought down by a hack. This means that less attention tends to be paid to the financial consequences for airlines of not only cyber attacks, but also less sinister IT network outages and the disruption to passengers caused by such events.

Most think of aviation as a high-tech and somewhat glamorous industry, but the reality is that margins are tight and risk management budgets are understandably focused on passenger safety. Moreover, the more established the airline, the more likely it is to be struggling with outdated legacy IT systems, upon which multiple newer systems are layered (rather than integrated in the truest sense), adding to the challenges of managing cyber risks.

Those challenges are multiplied exponentially by what is often called the "expanding network perimeter"; i.e. the technological interdependence between airlines and passengers booking via Global Distribution Systems (GDSs) and travel agencies, airport security, air traffic control, customs and immigration, baggage handling, catering, fuelling, and maintenance. Sharers of IT networks are only as secure as the weakest link in that network.

Evolving risk mitigation

For this reason, cyber insurers have traditionally been reluctant to cover airlines for business interruption losses caused by network outages sustained by any organizations other than the airlines themselves, and because of concerns over how losses can be aggregated over numerous airlines using the same technology providers. The number of carriers affected by one airport coming to a halt, whilst considerable, is dwarfed by the number of airlines dependent on any given GDS provider – only a handful of technology companies provide GDSs to the world's airlines. If one of the larger GDS providers were to be brought down, hundreds of airlines could be affected simultaneously.

If one of the larger GDS providers were to be brought down, hundreds of airlines could be affected simultaneously.

A further challenge for airlines is that insurance is all too often limited to only cyber attacks (in cyberinsurance parlance, "security failures"). Recent outages in the U.S. and UK should remind us that the potential for passenger disruption and airline income loss on a massive scale are just as likely to result from operational failures or negligence (i.e. "system failures") as from attacks.

In July 2016, a major U.S. carrier cancelled 2,300 flights, and thousands more flights were delayed, after a network router failed and back-up systems didn't kick in for 12 hours. Another large U.S. airline cancelled over 2,000 flights over three days in August 2016 as a result of malfunctioning power supply equipment tripping a transformer, leading to a loss of power at its headquarters. Its loss has been estimated at $150 million.

In January this year, a technical failure forced a contractor to cancel or delay a third of its contracted flights for three of the largest U.S. airlines in the course of a day. And just this May, one of Europe's largest flag carriers suffered a power failure in its primary data centre (reportedly as a result of a technician cutting the power and restoring it in an uncontrolled fashion) which led to 726 flight cancellations and delayed service for many more. The loss arising from that outage has been estimated at £80 million, but that figure does not account for long-term reputational damage.

Loss exposure

Of the airlines affected, only one is believed to have been insured for the losses in question, leading, it has been reported in the media, to a claim of between $60-100 million. This airline was one of the very few in the world which purchased what is generally known as system failure network business interruption cover. But most airlines still do not purchase stand-alone cyberinsurance and, even those that do, typically only buy a basic product covering business interruption loss arising from a security failure. Such cover would not be triggered in any of the above scenarios, because there was no suggestion of a cyber attack.

Most airlines still do not purchase stand-alone cyberinsurance and, even those that do, typically only buy a basic product covering business interruption loss arising from a security failure.

And the costs do not stop there. Airlines in certain territories are already subject to regulations requiring them to pay fines and/or compensation to passengers as a result of cancelled or delayed flights. In the U.S., substantial fines are payable by carriers to the Department of Transportation in the event of tarmac delays exceeding three hours, whilst in the European Union and many other territories, regulatory compensation is payable by airlines to passengers when flights are delayed or cancelled. In the case of the airline which sustained the May outage described above, compensation of up to £549 per person was payable to the affected passengers. That adds up to a staggering sum when one considers that 75,000 passengers are estimated to have been affected.

Another growing issue for airlines in the cyber arena is data protection regulation, given that airlines store a wide range of personal data which is shared with GDSs, travel agents, and frequent flyer program providers. As noted in our Summer 2016 edition of this brief, the European General Data Protection Regulation (GDPR) is heralding a far stricter data protection regime. Specifically, the GDPR introduces breach notification and non-compliance fines of up to 4% of annual global turnover (revenue) both for European airlines and any other carriers that have European-based passengers. The GDPR, which comes into effect on May 25, 2018, is only part of a wider global trend of stricter data protection legislation, with other countries introducing similar legislation.

Tailored approach

In the face of these challenges, the multi-layered and interdependent nature of IT systems in the airline industry suggests that companies will increasingly need a tailored risk transfer approach to cyber and related threats. Experience to date has only confirmed how various components of loss flowing from recent incidents would likely not be covered under a traditional cyber liability insurance policy.

"CyFly" is helping to address some of the gaps:

- Agreed value network interruption coverage in the event of an insured flight cancellation to simplify the loss quantification process,
- Network loss resulting from material interruption of the computer system of a broad range of third parties upon whom the airline is reliant for the provision of specified services, including passenger booking through global distribution services, verification of passenger identity, travel agency services, immigration and customs services, baggage handling and processing, runway and taxiing facilities, hangar facilities, aircraft maintenance facilities, fueling, catering and airport security.
- Frequent flyer program fraud coverage for direct financial loss from the theft, misuse or misappropriation of frequent flyer data by means of hacking of the insured's computer system by a third party.
- Civil aviation fines and compensation coverage for civil aviation fines that the insured is legally obligated to pay due to a flight cancellation or delay.

As technology continues to assume an ever-growing role in organizations' operating processes, it is critical to examine the potential effects of such changes, and to ensure that their risk transfer strategy adapts as necessary. This is especially true in the airline industry.

Contact

Jamie Monck-Mason
+44 20 3124 7240
Jamie.Monck-Mason@willistowerswatson.com

About Willis Towers Watson

Willis Towers Watson (NASDAQ: WLTW) is a leading global advisory, broking and solutions company that helps clients around the world turn risk into a path for growth. With roots dating to 1828, Willis Towers Watson has 40,000 employees serving more than 140 countries. We design and deliver solutions that manage risk, optimize benefits, cultivate talent, and expand the power of capital to protect and strengthen institutions and individuals. Our unique perspective allows us to see the critical intersections between talent, assets and ideas — the dynamic formula that drives business performance. Together, we unlock potential. Learn more at willistowerswatson.com.

willistowerswatson.com/social-media

WTW-GL-17-PUB-8053a1a

willistowerswatson.com