British Airways Data Breach – The First Major Aviation Loss under the GDPR

Aviation companies are no strangers to cyber threats. Airlines have been at the forefront of significant cyber attacks in recent years. This trend shows no signs of abating, as the recent British Airways (BA) data breach demonstrates.

On 6 September, BA revealed that more than 380,000 customers who had booked flights with the airline between 21 August and 5 September via BA's website and app had their credit card details stolen by hackers.

How Did the Attack Happen?

BA said that hackers did not break the airline's encryption but did not explain how hackers obtained customer information, merely stating that the breach was very sophisticated. The nature of the stolen data suggests that it happened during the payment clearing stage of transactions owing to poorly secured payment pages rather than the data being accessed in files kept by BA.

What Was Stolen?

During the two-week period, hackers had access to **names, street and email addresses, credit card numbers (in full), expiry dates, and security codes**.

- Saved credit card data on customer accounts were not affected (only data used in transactions during the stipulated 15 days were stolen)
- Payments made on PayPal or Apple Pay were not affected
- Bookings made outside the time frame, or through travel agents, were unaffected
- No travel or passport details were stolen

BA's Incident Response

BA immediately contacted customers once they realised that actual customer data had been compromised, apologising for the incident, and advising customers that "*If you believe you have been affected by this incident, then please contact your bank or credit card provider and follow their recommended advice.*"

BA contacted affected customers via email and announced on Twitter that they had experienced a data breach. The airline responded to customers on the platform, many of whom expressed that they had not been contacted yet, and those who had already received the notification email complained about the lack of detail and advice.

BA has stated that any direct financial loss suffered by a customer as a result of the breach would be compensated by the airline. This includes additional costs incurred in acquiring a new credit card (i.e. international postage fees).

Furthermore, BA will be offering a 12-month credit rating monitoring service to customers concerned about an impact to their credit rating, provided by specialists. BA's contact centres have also experienced high call volume following the breach.

We're here to empower results

To find out how Aon can enhance your cyber resilience, please contact:

Murray Wood
Head of Financial Specialties, Asia
+65 6645 0116
murray.wood@aon.com

Andrew Mahony
Regional Director, Financial Services & Professions Group
+65 6313 7080
andrew.mahony@aon.com

AON
Empower Results®

The Fallout

The morning after the breach was discovered, BA's Chief Executive appeared on BBC Radio 4's flagship Today programme. The airline also took out ads in national newspapers apologising for the breach. Shares in BA's parent, International Airlines Group, were down two percent during the afternoon trading the following day.

Following the breach, BA has been threatened with a £500 million ($650 million) class-action lawsuit in the U.K. court that contends BA has not gone far enough, and should be paying travellers "compensation for inconvenience, distress, and annoyance associated with the data leak". The action points to compensation rights in the General Data Protection Regulation (GDPR).

The country's Information Commissioner's Office said it had been alerted by BA, and was making enquiries. Under new GDPR data regulations, companies must inform regulators of a cyber attack within 72 hours. BA may yet prove to be an interesting test case on the enforcement of GDPR fines and penalties.

Coverage

The following losses (all of which have been or appear likely to be incurred by BA) may be claimed by BA under a cyber insurance policy:

Insurable Losses

- Forensic investigation costs
- Legal expenses – guidance in dealing with notification, regulatory investigations and possible third party claims
- Public relations expenses
- Notification expenses
- Credit card monitoring
- Call centre costs
- Liability to customers
- Liability to cardholders (reimbursing customers)

Cyber Risks Facing Aviation

The Aviation industry has suffered a number of major malicious and non-malicious losses which can be addressed by cyber insurance. BA itself experienced a significant system outage in 2017, allegedly owing to a power outage caused by an IT worker. Other airlines experienced similar events in 2016. All faced losses in the tens of millions of dollars. Airlines in Asia have also fallen victim to cyber attacks, involving website defacement, and access to sensitive frequent flyer data.

Airlines are highly vulnerable to both data breaches as well as business interruption losses. Disruptions to networks have the ability to cause significant financial and reputational damage to companies, and the exposure to sensitive personal data is a necessary prerequisite of serving customers, especially those customers whom are most loyal. As regulations continue to develop on a global scale, the repercussions airlines face from authorities as well as customers increase in severity.

Moving forward, airlines will inevitably continue to be a prime target for cyber attacks, and companies must improve their risk readiness and accept that cybersecurity risk management is a critical but necessary aspect of doing business across industries.

Moving forward, airlines will inevitably continue to be a prime target for cyber attacks, and companies must improve their risk readiness and accept that cybersecurity risk management is a critical but necessary aspect of doing business across industries.

How Aon Can Help

Aon treats every cyber risk placement as a unique opportunity to understand the specific exposures and concerns a client has, and to address those concerns accordingly through a bespoke insurance policy. Aon is the cyber insurance broker for three of Asia's leading airlines. This experience provides clients with unparalleled expertise in the Aviation sector.

Aon is also differentiated by its ability to provide comprehensive services addressing cyber resilience, including red team (ethical hacker) testing of systems, assessment and quantification of risk scenarios, tabletop cyber simulations, and incident response services.

Contact your Aon advisor to learn more about how we can help.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance. For further information on our capabilities and to learn how we empower results for clients, please visit: http://aon.mediaroom.com/

www.aon.com

Empower Results®