British Airways breach: Airline industry too lax on cybersecurity, experts warn

The news of a British Airways breach involving the payment data of 380,000 customers has led to harsh criticism of the airline industry's IT and cybersecurity efforts.

The fact that it took the airline 16 days to uncover the breach – an uncharacteristically long period for this kind of cybersecurity incident – has been a particular source of concern.

BA has also been plagued by IT issues over the last 18 months, while there have been two other high-profile breaches involving mainline airlines in the last six months.

"IT issues are not only affecting BA, but also in the wider airline industry," said Paul Farrington, head of EMEA at CA Veracode.

"Airlines have a duty to keep the planes in the air, and the majority of investment goes into that. However, recent outages show investment should also be directed at technology."

The growth of airline-targeted attacks

The airline industry is becoming an increasingly popular attack target. This is due the large quantities of data it handles, as well as the host of potential entry points for attackers as airlines roll out products such as apps and web portals.

"As airlines become ever more dependent on software, this creates a greater surface for hackers to attack and so it is no surprise that breaches of this scale are becoming commonplace," said Farrington.

"The British Airways breach once again sheds light on the difficulty companies have protecting the proprietary information of their customers that is their backbone," added Israel Barak, CISO at Cybereason.

"Collectively, this is a blow to our privacy and British Airways joins a growing list of organisations that have faced a knock down punch."

Recent data breaches in the airline industry

https://www.verdict.co.uk/british-airways-breach-airline-industry-too-lax-on-cybersecurity-experts-warn/

In the last six months there have now been three major breaches of leading airlines.

“In April, Delta revealed that data belonging to ‘hundreds of thousands’ of its customers had been compromised including credit card information,” explained Robert Wassall, data protection lawyer and head of legal services at ThinkMarble.

In this case no passport or ID data was involved, however the delay in identifying and reporting the incident was criticised.

“Delta only revealed the breach a week or so after it found out about it – and the breach had actually occurred 6 months previously,” added Wassall.

August saw a data breach involving the Air Canada app, which was particularly severed because it included identification data.

“Air Canada confirmed a data breach affecting 20,000 customers and said attackers may have accessed basic profile data, including names, email addresses and phone numbers — but also passport details, gender, dates of birth, nationality and country of residence. Fortunately, credit card data was not accessed,” he said.

British Airways becomes the third, with a breach that does involve personal and financial details, but not travel or passport data. In all three cases hackers took advantage of security flaws in the airline’s technology.

“Delta said the data was stolen after a security lapse at one of its third-party customer support providers. The Air Canada and BA breaches were via their mobile apps, and in the case of BA also its website,” said Wassall.

“All of these data breaches have created high risks to those affected. Not only is there the possibility of financial loss, there’s also a possibility that the attackers will know or be able to work out when people are going to be away from their homes – and so be vulnerable to break-ins.”

The British Airways breach and GDPR

It is not yet clear whether the British Airways breach will be subject to GDPR, but if it is, the fines could be significant.

“With GDPR now in full force the board at BA will have to consider their exposure to regulatory fines, especially when it took 16 days for the breach to be detected, and if the financial losses will outstrip what it would have cost to prevent the breach in the first place,” said Farrington.

However, it is important to note that GDPR has placed an onus on BA to report the breach while it continues to investigate what exactly happened due to the very short window the company has to report the breach in once it has been discovered.

This means that we will likely see more details emerge as the company’s investigation progresses.

https://www.verdict.co.uk/british-airways-breach-airline-industry-too-lax-on-cybersecurity-experts-warn/

“GDPR has placed us in a world where disclosure of data breaches are likely to occur before the full details of the attack are known,” explained Tim Mackey, technical evangelist at Synopsys.

“On the positive side, companies are highly incentivised to improve the level of security monitoring they perform. While to the travelling public, a two week window under which the attack wasn’t properly identified as such is alarming, the reality is that absent regulations like GDPR such incidents could go undisclosed for significantly longer.”