Data breaches and airlines: lessons learned!

Jeroen van Helden & Menno de Wijs

In February this year airline technology provider SITA was hit by a cyberattack targeting passenger data in its Passenger Service System servers. Several months later the personal data of thousands of ex-KLM employees were leaked due to a data breach at pension provider Blue Sky Group. In 2020, British Airways incurred a £20m fine following a data breach in which the personal details of about 400,000 customers were harvested by the attackers. What can and should airlines learn from these incidents?

SITA data breach

SITA is of course one of the largest aviation IT companies in the world, serving around 90% of airlines globally and helping them to manage reservations, ticketing, and aircraft departures via its in-house Passenger Service System. SITA suffered a major cyber attack on February 24, 2021, which involved hackers targeting its US-based servers that stored personal data records of a large number of flyers.

SITA's statements[1] did not detail what sort of data was targeted or stolen during the attack, nor how the attackers managed to get access to its network. What's certain is that the attack compromised the personal data of millions of airline customers. Various carriers issued their own statements about the breach, including Malaysia Airlines, Finnair, United Airlines, American Airlines and Air India. The breach also affected Singapore Airlines which, though not a direct customer of SITA, shared a limited set of data with partner airlines who were SITA customers.

Lesson 1: Data processor agreements

The SITA incident shows that airlines should not only focus on the security of their own network, but also on the security of their suppliers and partners. In other words, airlines should continually review security measures and procedures with their suppliers; requiring ISO certifications and clearly documented standards as a minimum, to be laid down in binding data processor agreements. Airlines should also scrutinise the purposes for which data is shared with partner airlines and minimise the sharing of data to what is relevant and necessary for the purposes concerned.

KLM Pension Fund

The Blue Sky Group manages the pensions of more than 53,000 former and current employees of KLM and other companies. Blue Sky Group manages, among others, the KLM General Pension Fund, KLM Cabine Pension Fund and KLM Flying Staff Pension Fund. In August this year, the company announced[2] that data had almost certainly been leaked from participants. This concerned, among

[1] https://www.sita.aero/pressroom/news-releases/sita-statement-about-security-incident/
[2] https://www.blueskygroup.nl/nl/nieuws/blue-sky-group-getroffen-door-datalek

other things, the names, policy and bank account numbers and pension amounts of participants who receive a pension, both relating to pensioners themselves and surviving dependents.

Lesson 2: Training and awareness
According to Blue Sky Group, the data breach originated after the attackers were able to gain access to a mailbox via a phishing email. Over 90% of all data breaches are the result of phishing emails. The risk that an employee clicks on a malicious link can hardly be brought down to zero, but can be reduced substantially by providing relevant training to staff, including through social engineering tests. Data protection authorities tend to view such awareness campaigns as an appropriate organisational security measure that any organisation working with large amounts of personal data should implement.

Another incident: 400.000 BA customers
As of 22 June 2018, users of British Airways' website were diverted to a fraudulent site. Through this false site, details of approximately 429,612 customers and staff were harvested by the attackers. This included names, addresses, payment card numbers and CVV numbers of 244,000 BA customers. Other details thought to have been compromised included the combined card and CVV numbers of 77,000 customers and card numbers only for 108,000 customers. Usernames and passwords of BA employee and administrator accounts as well as usernames and PINs of up to 612 BA Executive Club accounts were also potentially accessed.[3]

Lesson 3: Security measures
The UK Data Protection Authority, the Information Commissioner's Office (ICO), subsequently conducted an investigation and ultimately imposed a £20m fine on BA. Important to note is that BA was not fined for the occurrence of the data breach as such, but for a lack of security measures in place.

On the basis of the GDPR organisations are obligated to implement appropriate technical and organisational security measures to prevent data breaches. Such measures are not necessarily a guarantee against data leaks. A data breach may occur despite the fact that appropriate measures were in place, e.g. as a result of human errors or as a result of a sustained, targeted and sophisticated attack. In the BA case, the ICO concluded there were numerous measures BA could have used to mitigate or prevent the risk of an attacker being able to access its network. The BA case provides valuable guidance on security measures that every airline should implement as a minimum, including:

- limiting access to applications, data and tools to only that which are required to fulfil a user's role;
- undertaking rigorous testing, in the form of simulating a cyber-attack, on the business' systems;
- protecting employee and third party accounts with multi-factor authentication.

None of these measures, according to the ICO, would have entailed excessive cost or technical barriers, with some available through the Microsoft Operating System used by BA.

[3] https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-fines-british-airways-20m-for-data-breach-affecting-more-than-400-000-customers/

The ICO investigators also found that BA did not detect the attack on 22 June 2018 themselves but were alerted by a third party more than two months afterwards on 5 September. This was considered by the ICO to be a severe failing because of the number of people affected and because any potential financial harm could have been more significant. In other words, airlines should ensure they have adequate network monitoring in place.

Lesson 4: Representations

Finally, what's interesting in the BA case is that in June 2019 the ICO issued BA with a notice of intent to fine for a record penalty of £183m. As part of the regulatory process the ICO subsequently considered both representations from BA and the economic impact of COVID-19 on their business before setting a final penalty, which was then reduced by as much as £163m to £20m. The exceptional circumstances caused by the COVID-19 pandemic will (hopefully) not recur any time soon, but it shows the importance of putting up a solid legal defense against any fine (intended to be) imposed by a data protection authority.

More information

Would you like to know more about the legal aspects of IT security and data breaches? Feel free to contact our team.

Jeroen van Helden
Attorney at law
T: +31 (0)71 581 53 10
M: +31 (0)6 28 53 60 54
E: j.vanhelden@declercq.com

Menno de Wijs
Attorney at law
T: +31 (0)71 581 53 57
M: +31 (0)6 41 19 48 80
E: m.dewijs@declercq.com

This article appeared in the BARIN newsletter (edition 2021/21)