British Airways data breach fine: will it get off lightly?

Published 12-Jul-2019 by
Darren Wray

British Airways (BA) is one of the first organisations to have a major data breach since the General Data Protection Regulation (GDPR) came into force on May 25, 2018. The names and credit card information, including the CV2, of around 380,000 customers were stolen.

One or more people managed to gain access to BA's web servers and made changes to the website's source code. These changes allowed the information entered by BA's customers to be captured directly from the form on the BA website. They were packaged up before being sent to a website in Romania. This method is known as Magecart and has been something that cyber-security teams have been aware of and guarding their websites against since 2014.

This approach to stealing credit card information from websites is synonymous with card skimming. This is what seems like an old-fashioned attack method these days, but one that sometimes reappears, where someone adds an extra card reader to an ATM or card payment system. That allows the details to be captured from the magnetic stripe on the back of the credit or debit card, before sending the information, usually by Bluetooth, to the criminal, who will be parked nearby.

The fine

British Airways' parent company, International Airlines Group (IAG), which is the recipient of the proposed £183 million fine from the Information Commissioner's Office (ICO), has responded that the fine is disproportionate. There is not a set methodology for calculating a GDPR fine, but some of the factors can be established based on historical statements from the ICO in relation to other fines. The reality is, however, that in the current regulatory environment, which is becoming more assertive, BA may have got off lightly.

The fines criteria used by the ICO include:

- the size of the data breach (bigger is definitely worse);
- the type of data that has been lost in the breach (the more damaging to individuals, the higher the fines);
- the duration of the breach (longer is worse);
- how the organisation dealt with the breach (having a good breach plan and demonstrating preparedness is a real advantage); and
- the organisation's ability to demonstrate its compliance with regulation and to work with the regulator, which is an important factor and certainly appears to have reduced the size of the fine in the case of BA.

Many people will be aware that the technical limit for fines under the GDPR is the greater of 20 million euros or 4% of global annual revenue. In this case the regulator fined IAG £183 million, or 1.5% of its 2017 global revenue. If the fine had been as high as the 4% of revenues available under the EU regulation, therefore, this could theoretically have added hundreds of millions to the bill.

Lessons for financial services

This being the first fine from the ICO (although, with other big breaches having happened since, it is definitely not the last), it is natural that organisations in other sectors will ask what this fine means for their sector.

This action from the ICO clearly signals that it means business. The ICO has, with a single fine, more than tripled the GDPR fines levied across the rest of Europe (CNIL, the French data privacy regulator, previously held the record when it fined Google 50 million euros).

This is a strong message to the financial services sector, for which data privacy and protection, along with cyber security, is part of everyday business. It may mean any organisation from this sector will be held to a higher standard.

"The BA fine" will be appearing on the agenda of quite a few forthcoming board meetings, as firms digest the news and look to reassure themselves that they are doing all they can to avoid becoming — like BA — a negative headline around the world. The immediate response for some firms will be, to quote Corporal Jones from the UK's classic sitcom "Dad's Army": "Don't panic, don't panic!" They will be thinking very defensively.

After all, many firms have spent millions of pounds collectively on GDPR. A number of organisations, however, (including those in the financial services sector) believe they have done "just enough" and in many cases treated GDPR as a "one and done" project, rather than a compliance regime that has to be maintained continuously.

Boards and executives finding themselves in such a position may like to consider the following actions to reassure themselves about their organisation's GDPR risk profile.

• **Effective vendor management** is an often under-appreciated line of defence (the UK Financial Conduct Authority regards risk from third parties to be one of the greatest risk factors when it comes to cyber defence).

A good vendor management process will ensure that vendors are adhering to an organisation's data privacy and security standards. This is vital for companies protecting themselves against GDPR exposure. A firm can outsource the function but not the responsibility. This means that if a vendor loses some of the clients' personal data, the organisation is still responsible in the eyes of the ICO.

• **Ensure that the organisation "breach-ready"** As BA can attest, a breach incident can come out of the blue with little or no warning. The only way to ensure that the firm is ready for it is to maintain and test readiness. This is just as necessary as the fire evacuation drills that offices all over the world perform on a regular basis.

• **Change to technical environments** — and in some cases to business processes — have the potential to expose the firm to risks of a breach (both accidental and malicious). Firms will need to manage change carefully and should aim to include privacy and security by design. This is something that most organisations are still coming to terms with.

• **Having a well-structured subject access response (SAR) process** is important. This ensures that requests are dealt with as quickly and efficiently as possible to ensure that the time limits imposed by the GDPR are not breached.

• **Any personal data about people other than the data subject should be redacted**. There are many businesses that may unwittingly be accidentally committing a data breach in their response to a simple subject access request asking for a copy of their personal information. Such risks could be reduced by **hiring a data protection officer (DPO)**.

Not all firms need a full-time DPO (there are a few flexible, virtual DPO options out there). Many businesses do not have the natural skills or the bandwidth to hire a DPO, but the evidence is clear that those that do will have a distinct advantage when it comes to mitigating their data breach risks and exposures. This is only the end of the beginning for global data privacy regulation. A few years down the line businesses will look back fondly on the days when fines totalled in the low hundreds of millions and did not include nearly as much time in court or lawyer's fees.

Produced by Thomson Reuters Accelus Regulatory Intelligence 15-Jul-2019