KCS Group Europe

Air-fought convention

18th July 2019

British Airways has been handed a £183m fine for 2018's data breach, in what is a record penalty applied against a UK firm. After suffering the theft of customer details for 500,000 people over a four-month period between July and September last year, this fine is the first to be given under the new GDPR laws of 2018 and is seemingly indicative that the government is planning to practice what it preaches. But will this make a difference?

There can be no doubt that the Information Commissioner's Office is playing hardball with BA, levying if not quite the permissible 4 percent of turnover (which would be approaching £500m) then still an extremely high amount, but also no doubt that this is not only fair, but necessary. Indeed, for the first case brought under GDPR, this is a wake-up call to all businesses that the government is (finally) using its powers and is taking data breaches seriously.

Certainly, more seriously than BA, which arguably in its intention to appeal and its assertion that it is 'surprised and disappointed' by the ruling is still displaying blindness about just how serious a potential, or actual, breach can be. Much rests on its claim that there was no fraudulent activity arising from the theft. This quite staggeringly misses the point. Given that customers' personal information including addresses, email addresses and credit cards was appropriated, the (apparent) lack of fraud is only the best of a very bad range of scenarios, rather than something to be applauded. The fact that this data has been stolen the first place is the problem, and the attitude of 'nothing was done with it' is at best misguided and at worst actively damaging. We do not have protections in place only for when disasters do happen, but because they might.

Besides, the original thief of the data does not directly need to use it to benefit. Not only does the hack prove that the act can be carried out (whether with BA the ultimate targets or as an example), but the data can be sold on the dark web to third parties who will use it for their own ends. This is the supply chain in action again: for all those compromised, their existence on the BA database is a point of weakness, and therefore entire lives can be affected by one point of failure.

This issue is set in the wider context that firms in the UK remain largely toothless to take the fight to the bad actors and actually attempt to retrieve the data (which would be the ideal), but serves as a reminder that prevention is better than cure: the tougher security measures BA implemented afterwards would have served much better before.

BA may yet win their appeal, but arguably in order for this case to have impact the punishment must stand. This is a clear case of an organisation not looking after customer data, irrespective of whether anything was actually done with it. Data is the most important currency of the digital age and the failure to take care of it properly is the rationale, as well as the lesson, behind the fine. It is not a question of being proportional to damage caused but proportional to potential damages arising from organisational failings. If the GDPR rulings (and implications) are taken as seriously by the companies they are trying to benefit as much as the now on-message authorities, then there may yet be clear skies ahead.