GlobalResearch
Center for Research on Globalization

Airlines at a Time of Crisis: Patterns of Compromise: The EasyJet Data Breach

By Dr. Binoy Kampmark
Global Research, May 24, 2020
Region: Europe
Theme: Intelligence, Law and Justice

It has been a withering time for the airlines, whose unused planes moulder in a gruelling waiting game of survival. The receivers are smacking their lips; administration has become a reality for many. Governments across the globe dispute what measures to ease in response to the coronavirus pandemic; travel has been largely suspended; and the hope is that some viable form will resume at some point soon.

For the low-cost airline EasyJet, a further problem has presented itself. Earlier in the week, the company revealed that it had "been the target of an attack from a highly sophisticated source", resulting in a data breach affecting nine million customers. Of those, 2,208 customers ("a very small subset", as the company wished to emphasise) had had their credit and debit card details "accessed".

The UK's Information Commissioner's Office had been informed about the incident but the company only revealed this catastrophic lapse in data security to individuals, as it told the BBC, "once the investigation had progressed enough that we were able to identify whether any individuals had been affected, then who had been impacted and what information had been accessed."

EasyJet were also quick to douse the fires of this grim chapter in data insecurity.

> "There is no evidence that any personal information of any nature has been misused, however, on the recommendation of the ICO, we are communicating with the approximately nine million customers whose travel details were accessed to advise them of protective steps to minimise any risk of potential phishing."

This phishing risk entails that opening any suspicious email purporting to be from EasyJet is simply a risk not worth taking. Naturally, the company will have to inform, and have informed customers of that very risk, resulting in a peculiar circularity: Who to believe and what enables the recipient to detect the suspicious? As digital privacy expert Ray Walsh opines, "Anybody who has ever purchased an EasyJet flight is advised to be extremely wary when opening emails from now on."

For the company's part, customers whose credit card details were compromised have received an email with a unique code, ostensibly to access services provided by a third party. A call centre to deal with concerns arising from the hack has also been established, though service on that has been typically sloppy.

Airline companies have a rather patchy record in the field of data security. In the cybersecurity department, they seem to be rather thin, a failing that matches a global tendency. (A 2018 report suggested a shortage of some 2.93 million.) The implications to both airline companies and aviation infrastructure have been of such magnitude as to prompt warnings that it is merely a matter of time before aircraft are themselves the subject of cyber-attack.

The honour board on compromised customer data is a long one. Cathay Pacific Airways experienced an attack on the scale of that of EasyJet, with a hacker accessing the personal information of 9.4 million customers over a four-year period. This was also a case that interested the ICO, resulting in a pre-General Data Protection Regulation fine of £500,000. The ICO investigation revealed that the airline lacked adequate security controls to ensure the integrity of passenger data within internal IT systems. This "resulted in the unauthorised access" to "passengers' personal details including: names, passport and identity details, dates of birth, postal and email addresses, phone numbers and historical travel information."

Cathay Pacific's systems were penetrated via an internet server enabling the installation of data harvesting malware. It did not help that the data storage regime in place was weak and complacent. Back-up files were not password protected; internet-facing serves were unpatched; the presence of inadequate and outdated anti-virus protection software was noted.

British Airways was less fortunate in being fined £183 million in 2019 by the ICO, armed with the more punitive powers of the GDPR, for failing to take adequate steps in protecting the personal information of some 380,000 customers. The 2018 compromise of data took place through bookings made on its website (ba.com) and the British Airways mobile app over the course of a 15 day period. As with EasyJet, the company adopted a strategy of understating the effect of it all. Yes, personal details had been stolen, including the names, addresses and financial information of customers, but those cheeky hackers did not make away with passport or travel details. And, before anybody should get too excited, the cyber incident was, according to a spokesperson for British Airways, "data theft, rather than a breach".

None of this impressed the Information Commissioner Elizabeth Denham. "People's personal data is just that – personal. When an organisation fails to protect it from loss, damage or theft, it is more than an inconvenience. That's why the law is clear – when you are entrusted with personal data you must look after it."

Not to be left out, Air Canada also confirmed a data breach on its mobile app in August 2018, though the scale was a more modest 20,000 individuals. One defective feature of the airline's operating systems stood out: a mediocre password policy accepting only letters and numbers.

Such patterns of compromise are all too common in the commercial aviation industry, but EasyJet's Chief Executive Officer Johan Lungren claims to be wiser after the fact. "Since we became aware of the incident, it has become clear that owing to COVID-19 there is heightened concern about personal data being used for online scams." Pressed by the ICO, "we are contacting those customers whose travel information was accessed and we are advising them to be extra vigilant particularly if they receive unsolicited communications." A fine of some magnitude is expected.

*

Note to readers: please click the share buttons above or below. Forward this article to your email lists. Crosspost on your blog site, internet forums. etc.

Dr. Binoy Kampmark *was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. He is a frequent contributor to Global Research and Asia-Pacific Research. Email: bkampmark@gmail.com*
