The Biggest Data Breach Fines: Don't Give Your Business a Fright

Cyberattacks, paper-based breaches and data thefts, enabled by weak security, cover-ups and avoidable mistakes have cost companies more than just their reputation, with data breach fines extending into the billions.

Here we take a look at the biggest data breach fines from around the world – thus far – and essential steps you can take to ensure your business remains protected from crippling monetary penalties and irreparable reputational damage.

1 EQUIFAX - £447 MILLION

In 2017, US credit reporting agency, Equifax, lost the personal and financial information of some 150 million users following an unpatched framework in one of its databases. In July 2019, the firm agreed to pay $575M – potentially rising to $700M – in a settlement with the FTC and CFPB.

2 BRITISH AIRWAYS - £179 MILLION

In July 2019, British Airways was fined $230M – the largest GDPR fine to date – by the ICO, after a malicious hacker group diverted user traffic to a fraudulent site and used card skimming scripts to harvest the confidential data of more than 500,000 customers.

3 UBER - £115 MILLION

In 2016, ride-hailing app, Uber, suffered a breach which compromised the data of some 600,000 driver and 57 million user accounts. Instead of reporting the incident, the company paid the perpetrator $100,000 to keep the hack under wraps. But this proved to be a costly decision, with the firm later fined $148M in 2018.

4 MARRIOTT INTERNATIONAL - £96 MILLION

Shortly after the astronomical fine received by British Airways, Marriott were the next corporation to fall victim to the long arm of the ICO. In July 2019, the hospitality giant was hit with a $124M fine, following a data breach which compromised the names, payment information, addresses, phone numbers and email of some 500 million customers.

5 YAHOO - £66 MILLION

Back in 2013, Yahoo suffered a substantial security breach that compromised the confidential data of its entire database – some 3 billion accounts! Rather than reporting the incident, the company chose not to disclose the data breach for 3 years, eventually resulting in a fine of $35M from the SEC and a class action lawsuit that was settled for a further $50M.

So, as you can see, no business – regardless of size – is safe from the fines and reputational damage that inevitably incurs from a data breach. But it's not just the large corporations who must comply with regulations, like GDPR.

Companies, of all shapes and sizes, must adhere to these strict rules and regulations in order to protect the confidential data of customers, clients and ultimately, your own business.

Here's a few simple steps to help you protect your business.

Document the data you hold:
Identify where personal data is stored in both physical and online files.

Communicating privacy information:
Upload an updated privacy policy and circulate policies to staff.

Increase cyber security:
Keep everything up-to-date and password protected.

Protect it:
Use a document management process so data is secured from creation to disposal.

Record data breaches:
If a breach occurs and it's likely there will be a risk, you must notify the appropriate bodies.

Be prepared:
In the case of a data breach, have an effective response plan in place.

Destroy it:
Have a formal procedure for the secure destruction of documents containing sensitive information or introduce a Shred-it All Policy so that all documents are securely destroyed.

For peace of mind, contact Shred-it® today
0800 197 1164 | shredit.co.uk

Shred-it® is a Stericycle solution. © 2019 Shred-it® International. All rights reserved.

Shred-it®