

## Yahoo data breach

- What types of data were affected?

The database contained names, phone numbers, password challenge questions and answers and, crucially, password recovery emails and a cryptographic value unique to each account

- What happened?

- 2 data breaches in 2013 and 2014
- 3 billion user accounts affected in total
- Spear phishing email attack used. May have been sent to many employees, but this is unknown (Martyn Williams, 2017).
- Spear phishing is a targeted attack against a named employee. The hacker may have personal information about the employee gained through social engineering methods, which assists the hacker in appearing legitimate to the employee. The employee then clicks on a link, which allows the hacker to gain access to unauthorized systems
- The hacker looked for two main functions: Yahoo's user database and the Account Management Tool, which is used to edit the database (Martyn Williams, 2017).
- He then installed a backdoor on a Yahoo server that would allow him access, and in December he stole a backup copy of Yahoo's user database and transferred it to his own computer (Martyn Williams, 2017).

- Who was responsible?

Aleksey Belan, a Latvian hacker hired by the Russian agents (Martyn Williams, 2017).

- Were any escalation(s) stopped - how?

No, the first hack took place in 2013 and another in 2014. There was insufficient monitoring to detect the first breach, thus allowing the hackers to perform a second, more deadly breach (*Yahoo data breach: NCSC response - NCSC.GOV.UK*, 2017).

Yahoo's investigation was not thorough and remedial action and response was poor. Senior execs did not comprehend the magnitude of the hack and failed to investigate further. Only 26 users were initially notified (Kan, 2017).

- Was the Business Continuity Plan instigated?

No downtime was reported as a result of the hack, and as such, the BCP did not need to be implemented.

- Was the ICO notified?

Unknown if the breach was reported prior to disclosure to affected individuals, however yahoo was fined 250 thousand pounds as a result (*Yahoo fined £250k for data breach - The Data Privacy Group*, no date).

This breach predates the GDPR regulations and was investigated under the data protection act of 1998. If GDPR were to be enforced, the fine would be a lot higher

- Were affected individuals notified?

Users were informed 2 years after the attack. Erroneously underreported and then corrected a year later

- What were the social, legal and ethical implications of the decisions made?

Decreased sales price to Verizon of \$4.8 billion, reduced by \$350million (Kharpal, 2017).

Yahoo fined 35million for delaying notification to affected users

50 million dollar total settlement for 200 million affected users in US and Israel based on time spent dealing with the breach, equating to 375 dollars max each. (requires proof of time spent)(*Remember the 2013 Yahoo Data Breach? The Company May Owe You \$375 | Inc.com*, no date).

Marissa Meyer, CEO stepped down partly as a result of the breach (Kharpal, 2017).

Kan, Mi. (2017) 'Yahoo execs botched its response to 2014 breach, investigation finds', Cso. Available at: <https://www.csoonline.com/article/3176181/yahoo-execs-botched-its-response-to-2014-breach-investigation-finds.html> (Accessed: 15 October 2021).

Kharpal, A. (2017) *Verizon completes acquisition of Yahoo as Marissa Mayer resigns*, CNBC. Available at: <https://www.cnbc.com/2017/06/13/verizon-completes-yahoo-acquisition-marissa-mayer-resigns.html> (Accessed: 15 October 2021).

Martyn Williams (2017) *Inside the Russian hack of Yahoo: How they did it* | CSO Online. Available at: <https://www.csoonline.com/article/3180762/inside-the-russian-hack-of-yahoo-how-they-did-it.html> (Accessed: 15 October 2021).

*Remember the 2013 Yahoo Data Breach? The Company May Owe You \$375* | Inc.com (no date). Available at: <https://www.inc.com/minda-zetlin/yahoo-data-breach-50-million-lawsuit-settlement-account-holders-375.html> (Accessed: 15 October 2021).

*Yahoo data breach: NCSC response* - NCSC.GOV.UK (2017) NCSC. Available at: <https://www.ncsc.gov.uk/news/yahoo-data-breach-ncsc-response> (Accessed: 15 October 2021).

*Yahoo fined £250k for data breach* - The Data Privacy Group (no date). Available at: <https://thedataprivacygroup.com/blog/yahoo-fined-for-data-breach/> (Accessed: 15 October 2021).