Breach Analysis Case Study

Yahoo

The Yahoo data breach is one of the largest and most significant cybersecurity incidents in history. It involved two separate breaches:

- 2013 Breach – Affected all 3 billion Yahoo accounts worldwide.
- 2014 Breach – Affected 500 million accounts and was later linked to Russian state-sponsored hackers.

Yahoo failed to detect the breaches at the time and only disclosed them in 2016, years after the attacks occurred.

Breach Checklist

Category	Details
Types of Data Affected	Names, email addresses, phone numbers, dates of birth, hashed passwords (MD5), security questions & answers (some unencrypted)
What Happened?	Two breaches (2013 & 2014), affecting 3 billion & 500 million accounts. Weak encryption & poor monitoring allowed attackers to extract data undetected.
Who Was Responsible?	2013: Unknown hackers; 2014: Russian state-sponsored hackers. US DOJ charged Russian intelligence officers & hackers.
Were Escalations Stopped?	No. Breaches went undetected for years. No effective security measures prevented escalation.
Was the Business Continuity Plan Used?	No clear evidence of a robust BCP. The slow response suggests poor incident response planning.
Was the ICO Notified?	Yes, but only after Yahoo publicly disclosed the breach in 2016. Possible GDPR non-compliance due to delayed reporting.
Were Users Notified?	Yes, but the delay (2016) increased security risks for affected individuals.
Social, Legal & Ethical Implications	Social: Loss of trust, risk of identity theft. Legal: $35M SEC fine, $117.5M lawsuit settlement, £250K ICO fine. Ethical: Delayed disclosure, weak security, prioritising reputation over users.
Mitigations as ISM	Strong encryption, MFA, security audits, network monitoring, access control, incident response planning, timely breach disclosure, security training.

Abbreviations

BCP – Business Continuity Plan
ICO – Information Commissioner's Office
MD5 – Message-Digest Algorithm 5
DOJ – Department of Justice
ISM – Information Security Manager
PoLP – Principle of Least Privilege
GDPR – General Data Protection Regulation
MFA – Multi-Factor Authentication
SEC – Securities and Exchange Commission

Was MD5 Already Bad Practice?

MD5 was designed in 1991 and officially deprecated by 2004 due to serious vulnerabilities. Cryptographic researchers found collision attacks (where two different inputs can produce the same hash), making MD5 unsuitable for security-sensitive applications. Tools for cracking MD5 hashes became widely available, meaning passwords hashed with MD5 could be broken within seconds.

Yahoo was still using MD5 at the time of the breach 10 years after it had been depreciated.