Equifax Data Breach

Case study

Sergei Lebedev

This document will discuss the Equifax breach of 2017. The breach occurred due to a vulnerable component in Equifax software, which was not patched promptly. (Fruhlinger, 2020)

What types of data were affected?

Customers’ personal information: names, addresses, dates of birth, social security numbers, drivers’ licenses, as well as credit card information (Fruhlinger, 2020).

What happened?

A vulnerable component was used in one of Equifax's services and not updated in a timely manner.

This allowed the adversaries to access corporate systems in March 2017 and access customers' personal data starting May 2017.

The attack was not discovered until late July 2017 due to expired subscription for the detection software. Information about the breach was publicised in September 2017

(Fruhlinger, 2020; Breachsense, 2024).

Who was responsible?

Members of Chinese military were charged for the data breach (U.S. Department of Justice, 2020).

Were any escalation(s) stopped - how?

After the intrusion was detected in July 2017, the attackers' access to the corporate systems was blocked by the information security department of Equifax. Later the website with the initial vulnerability was taken down to prevent further attacks (U.S. Government Accountability Office, 2018).

Was the Business Continuity Plan instigated?

It is unclear whether such plan was in place. However, Equifax had hired a cybersecurity firm Mandiant to conduct an investigation in August shortly after the breach was discovered (Mozilla, no date).

Extensive logging implemented in the corporate systems allowed to understand the scope of the data breach and the affected individuals (Digital Uppercut, 2019).

At the same time, there was a delay before the information was published, as well as issues with communicating the breach (Newman, 2017).

Was the ICO notified?

Equifax Ltd, the UK branch of Equifax had informed the Information Commissioner’s Office shortly after the information was publicised by the parent company (Information Commissioner’s Office, 2018, p. 24).

Were affected individuals notified?

Equifax made the information about the breach public in September 2017 and set up a resource for its customers to determine whether they were affected (Fruhlinger, 2020).

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

The company's relaxed approach to addressing the data breach resulted in reputational losses and led to legal consequences for Equifax: the firm eventually entered a settlement in a class action lawsuit in the United States and agreed to pay over 500,000 million USD to affected parties (Mozilla, no date).

Additionally, Equifax lost a government contract with the U.S. Internal Revenue Service (IRS), and the breach prompted the IRS as well as some other U.S. government agencies to require their subcontractors to notify the agencies about any data breaches in a timely manner. The UK branch Equifax Ltd was fined for the amount of 500,000 GBP for non-compliance with the Data Protection Act of 1998 (Information Commissioner's Office, 2018, p. 26).

The incident sparked the discussion around implementing more strict data processing regulations in the United States and the European Union (Breachsense, 2024).

If you had been the ISM for the organisation you selected, what mitigations would you have put in place to stop any reoccurrences?

Improve the management of software development and procurement of cybersecurity software

The employees at Equifax were aware of the vulnerability in their software, but either the information was not delivered to the person responsible for the resource to become the entry point for the attack, or they failed to implement the fix. A week later, a security scan did not reveal the still vulnerable component (U.S. Government Accountability Office, 2018, p. 15; Fruhlinger, 2020).

This could have been avoided by implementing a more strict process for tracking security-related tasks with clear assignees and deadlines. The vulnerable dependencies can be monitored and patched automatically with tools like GitHub's Dependabot to minimise human involvement in the process (GitHub, 2025a, 2025b).

The software that could detect malicious network traffic was misconfigured and not renewed. Almost immediately after this issue was identified and fixed, the data breach was discovered (U.S. Government Accountability Office, 2018, p. 14). This highlights the need for the policy to keep security software up to date and monitor its status regularly.

Develop an incident response plan

The actions that followed, such as delayed announcement about the breach, as well as its poor communication (Newman, 2017), indicate the lack of an up to date incident response plan. An incident response plan must be prepared in advance to guide the mitigation effort for security incidents: how to detect, analyse, contain, and neutralise the threats, as well as what actions to take in the aftermath (Bandos, 2016).

These measures, while simple, could have prevented the breach or minimised its impact. It is reasonable to assume that should the original breach in March 2017 have been detected and contained, the eventual data breach that affected millions of Equifax's customers would not happen.

References

Bandos, T. (2016) The Five Steps of Incident Response. Available at: https://www.digitalguardian.com/blog/five-steps-incident-response (Accessed: 28 July 2025).

Breachsense (2024) Equifax Data Breach Case Study: Causes and Aftermath. Available at: https://www.breachsense.com/blog/equifax-data-breach/ (Accessed: 20 August 2025).

Digital Uppercut (2019) 'Equifax Breach and Settlement: What Equifax Did Right', 22 August. Available at: https://www.digitaluppercut.com/equifax-did-right/ (Accessed: 20 August 2025).

Fruhlinger, J. (2020) 'Equifax data breach FAQ: What happened, who was affected, what was the impact?', CSO Online, 12 February. Available at: https://www.csoonline.com/article/567833/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html (Accessed: 3 August 2025).

GitHub (2025a) About Dependabot alerts, GitHub Docs. Available at: https://docs-internal.github.com/_next/data/5rlFtOcDABhbJNMFHoG3O/en/free-pro-team%40latest/code-security/dependabot/dependabot-alerts/about-dependabot-alerts.json?versionId=free-pro-team%40latest&productId=code-security&restPage=dependabot&restPage=dependabot-alerts&restPage=about-dependabot-alerts (Accessed: 20 August 2025).

GitHub (2025b) About Dependabot security updates, GitHub Docs. Available at: https://docs-internal.github.com/_next/data/5rlFtOcDABhbJNMFHoG3O/en/free-pro-team%40latest/code-security/dependabot/dependabot-security-updates/about-dependabot-security-updates.json?versionId=free-pro-team%40latest&productId=code-security&restPage=dependabot&restPage=dependabot-security-updates&restPage=about-dependabot-security-updates (Accessed: 20 August 2025).

Information Commissioner's Office (2018) 'Data Protection Act 1998. Supervisory Powers of the Information Commissioner. Monetaty Penalty Notice to Equifax Ltd'. Available at: https://web.archive.org/web/20200224165906/https://ico.org.uk/media/action-weve-taken/mpns/2259808/equifax-ltd-mpn-20180919.pdf (Accessed: 20 August 2025).

Mozilla (no date) Equifax data breach: A look at how it happened, Mozilla. Available at: https://www.mozilla.org/en-US/products/monitor/equifax-data-breach/ (Accessed: 20 August 2025).

Newman, L.H. (2017) 'All the Ways Equifax Epically Bungled Its Breach Response', Wired, 24 September. Available at: https://www.wired.com/story/equifax-breach-response/ (Accessed: 20 August 2025).

U.S. Department of Justice (2020) Office of Public Affairs | Chinese Military Personnel Charged with Computer Fraud, Economic Espionage and Wire Fraud for Hacking into Credit Reporting Agency Equifax | United States Department of Justice. Available at: https://www.justice.gov/archives/opa/pr/chinese-military-personnel-charged-computer-fraud-economic-espionage-and-wire-fraud-hacking (Accessed: 20 August 2025).

U.S. Government Accountability Office (2018) 'Data Protection: Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach'. Available at: https://www.gao.gov/assets/gao-18-559.pdf (Accessed: 20 August 2025).