Pre-course study

Institute of Data / UTS

‘Understanding Cyber Security’

EQUIFAX case study

Owner:	Laurent Gatefait
Created:	25/05/2025
Last Modified:	30/05/2025

Table of Contents

EXECUTIVE SUMMARY

This case study of the EQUIFAX data breach attempts to outline the root cause of the incident, lessons for organisations, and recommendations.

Two reports; The GAO report to Congress summarizes the events regarding the breach and the steps taken by Equifax, and actions by federal agencies to respond to the breach; and the Committee on Oversight and Government Reform EQUIFAX breach report details the root causes, severe technical vulnerabilities, systemic failures, complacencies, massive accountability oversight, and poor mediation actions. Crucially, they provide recommendations covering technical aspects, organisational practices, communication and regulation.

Other articles and sources highlight the breach's consequences for Equifax and impact to Equifax, the industry and public at large, including massive economic costs, legal impacts, congressional scrutiny, governmental reforms and geo-political repercussions.

INTRODUCTION

EQUIFAX, a major credit reporting agency in the US, had their systems breached in March 2017, compromising the personal information of 148 million people (Committee report). This breach is widely considered as one of the most significant cybersecurity incidents in history because of its scope and severity, exposing sensitive data with serious consequences. It disclosed private data (PII) such as social security numbers, birth dates, addresses, and even credit card information in some cases.

Major data breaches and identity theft have become increasingly frequent and damaging, the infamous Equifax breach is just one of many. Other credit reporting agencies like Experian, and TransUnion have also failed to safeguard sensitive consumer data, with incidents exposing millions of records. Major breaches at companies like Yahoo, Target but also in Banks, Education, Healthcare have further highlighted the growing threat affecting millions annually, often leading to tax and credit card fraud, with enormous economic costs.

DISCUSSION

Significance of the study

The study and its reports served as a monumental wake up call for data protection at levels; public, government, and especially corporations.

Now adding the evermore interconnectivity and complexity of our digital age (eg IoT, Cloud Platforms), and the adoption of AI, the breach emphasises the ongoing and growing importance of Cyber protection as a core and critical business function.

In a larger context, the global economic impact of cybercrime is of 6 trillion USD per year and was projected to reach $10.5 trillion annually by 2025, with the cost of cyberattacks increasing significantly year-over-year (Cybersecurity Ventures 2020 reports). Although spending estimates vary, Statista expects annual spending to continue rising by an average of $17 billion per year, reaching $272 billion by 2029 (CyberCrime Magazine, 2020).

Root Cause

The root cause of the incident was a combination of failures in technical, process, individual and corporate responsibilities and accountabilities. The two reports along with other sources note:

1. **Unpatched Software Vulnerability:**
    - A known vulnerability in Apache Struts (CVE-2017-5638) was not patched.
    - Despite internal alerts, critical systems like the Automated Consumer Interview System (ACIS) were not updated.

2. **Expired Security Certificate:**
    - The breach went undetected for 76 days because a key network monitoring tool's SSL certificate had been expired for 19 months.

3. **Poor IT Management and Structure:**
    - Lack of clear responsibility and accountability in Equifax's IT department.
    - More than **300 expired security certificates** indicated systemic neglect.
    - An internal audit had previously identified over 8,500 unresolved software vulnerabilities, yet the company failed to address these issues promptly. (Seven Pillars Institute)

4. **Legacy Systems and Complexity:**
    - Equifax's systems were a patchwork of **legacy applications**, making security oversight difficult.
        i. Lack of segmentation between systems to avoid attak expansion
        ii. Lack of File Integrity Monitoring
        iii. Shared admin file systems
        iv. Web server logs retained for only short periods
        v. Lack of software inventory
    - A rapid acquisition strategy increased data volume and complexity without proportional security enhancements.
    -
5. **Leadership Accountability**:
    - Serious Gaps between IT Policy Development and Execution
    - the CIO, CSO, CEO and senior IT executive failing to adequately prevent and manage the breach, made difficult because of accountability gaps in the IT management org structure (according to the Commission report).

RESULTS & REPERCUSSIONS

The the fallout and ramifications of the investigations were wide ranging, including company misconduct leading to dismissals, regulatory scrutiny, additional congressional hearings, and lawsuits among others:

- **EQUIFAX cost** in cleanup estimated at $1.4 billing (BankInfo Secutrity)
- **Leadership Changes** in EQUIFAX :CIO, CSO, and CEO Richard Smith all resigned or retired (Committee report)
- A senior IT executive was **terminated** for not forwarding an email about the Apache Struts vulnerability. (Committee report)
- **Drop of 18% in Stock value** for Equifax at the time the breach was made public (Fortune)
- Chargers for the CIO **for insider trading** (US Attorney's Office) in June 2019
- The initial breach resulted in **investigations** by local, state and federal authorities:
    a. Federal Trade Commision (FTC)
    b. Consumer Financial Protection Bureau (CFPB)
    c. Congress
    d. UK and Canadian governments
    e. Federal Bureau of Investigation (FBI)
- Equifax faced **lawsuits and settlements**. In 2019, the company agreed to a $700 million settlement with the Federal Trade Commission (FTC) and other regulators.
- **Allegations**: the Senator Elizabeth Warren report details how Equifax prioritized profits over consumer data security (motivated by lucrative government contracts)

- **Regulations and reform** (Committee report):
    a. Reform the industry by giving consumers control over their credit reports
    b. Improve Breach Notification
    c. Limit the Use of Social Security Numbers by Private Companies
    d. Enact baseline privacy legislation and establish a Data Protection Agency
- Crucial lessons on private data protection for **consumers, corporations** and the Cyber Security **industry** as a whole with the story going viral in the online community

According to a Bloomberg Businessweek analysis, the breach progressed from initial access to a more advanced, organised attack, indicating a handoff from entry-level hackers to a sophisticated team—a hallmark of nation-state operations. “China Chopper,” a well-known web shell (a type of malicious software for maintaining remote access) that has a Chinese-language interface was used.

Attackers are usually motivated by financial gain, as the stolen personal data could be sold on the black market or used for identity theft. However no such personal data was found on the darkweb pointing to state espionage. Evidence of targeting individuals also suggests motives beyond profit, possibly for espionage and intelligence gathering.

Eventually FBI involvement concerned with national security threats resulted in four Chinese military members being charged by the US government in February 2020 (FBI), which underscores how grave and far reaching the consequences of poor data protection can be.

LESSONS LEARNT & RECOMMENDATIONS

Cyber attacks are projected to increase as consumers, businesses and products digitalise and go online more (World Economic Forum).

With the addition of improved and accessible AI tools, threats and attacks are set to increase, aiding attackers in automation, scalability and sophistication of the attacks.

All organisations are at risk, however, small to medium businesses whose capacity and budgets restrict them from large investment, and also their lack of knowledge, are more exposed. Cyber attackers are increasingly aware of this gap and make SMBs an increasing target. Cybercrime magazine notes “More than half of all cyberattacks are committed against small-to-midsized businesses (SMBs), and 60% of them go out of business within six months of falling victim to a data breach or hack.”

As threats are projected to increase, the two Equifax reports provide crucial practical recommendations and standards for individuals, corporations of all sizes, and authorities. This, along with other recommendations from the online community can be summarised below:

- **Public risk & awareness:** consumers continue to be exposed by cyber threats putting them at risk of identity theft, used for tax fraud, financial fraud, and medical identity theft. The public needs to remain vigilant when interacting with companies and online platforms. Tools like Google's darkweb search tool allows you to create a monitoring profile with various data inputs (eg email, telephone, address) to monitor, identify which sites have had leaks with your info in it, and how to take steps to protect your data.

- **Organisations risk & awareness**: organisations need to understand the heightened risks of handling consumers' private data. Small businesses are more susceptible and need to be educated. Educational programs for SMBs could be developed by local or state authorities. In Australia both the eCommisonar site and the https://www.actnowstaysecure.gov.au/ sites can be of good resource for both individuals and businesses.

- **Implement Robust Patch Management Processes**: organisations should establish and enforce comprehensive patch management policies, ensuring that all systems are regularly updated and vulnerabilities are addressed promptly,

- Better **system update processes** to ensure no security gaps with legacy or newly integrated systems.

- **Improve Incident Detection and Response:** organisations should invest in advanced monitoring tools and establish clear incident response protocols to detect and mitigate security incidents swiftly.

- **Transparent Communication:** the incident was made worse by Equifax's inadequate communication with affected individuals and regulatory bodies by senior members of staff. Organisations must develop clear communication strategies to inform stakeholders about security incidents promptly and transparently, maintaining trust and compliance.

- **Data Security Training** for staff members handling sensitive data reiterating the importance of processes, protocols, compliance and frameworks for data protection

- **Leadership accountability and responsibility:**
    a. Having an **adequate IT management structure** to ensure no accountability gaps.
    b. Ensuring IT policies are properly executed - by regular auditing for example.

- **Cybersecurity as a Core and Critical Business Function:** organizations should prioritize Cyber security as an important necessary investment, to continuously and regularly monitor, review, protect all aspects of data security.

- **Regulatation**: More regulation around data security laws and standards can be implemented by regulatory bodies to enforce and review best practices

- **Reduce the use of Social Security Number:** the reliance on one identifier makes for greater risk if SSNs are exposed.

- **Madiant** (Equifax's third party security consulted analysts) provided a detailed list of technical recommendations soon after the breach:
    a. Enhance vulnerability scanning and patch management processes and procedures;
    b. Reduce the scope of sensitive data retained in backend databases
    c. Increase restrictions and controls for accessing data housed within critical databases;
    d. Enhance network segmentation, to restrict access from internet facing systems to backend databases and data stores;
    e. Deploy additional web application firewalls and tuning signatures to block attacks;
    f. Accelerate the deployment of file integrity monitoring technologies on application and web servers;
    g. Enforce additional network, application, database, and system-level logging;
    h. Accelerate deployment of a privileged account management solution;
    i. Enhance visibility for encrypted traffic by deploying additional inline network traffic decryption capabilities;
    j. Deploy additional endpoint detection and response agent technologies; and
    k. Deploy additional email protection and monitoring technologies

CONCLUSION

Being vigilant and taking proactive steps to safeguard against cyber attacks has never been so paramount. The Equifax data breach serves as a critical lesson for robust cybersecurity practices and an example of the grave consequences of neglecting them.

The reports highlight the wide scope of areas to improve data security; from technical, technical process, organizational frameworks, communication, legal and policy.

Individuals, organizations small and large, can learn from this incident to strengthen their security frameworks, processes, accountabilities, response capabilities and be better prepared when they happen. Not only is this important for individuals and organizations, but protecting sensitive data also involves government agencies under attack from national security threats and maintaining public trust.

As Cyber attacks continue to grow in frequency, scope and complexity due to rapidly evolving environments and tools like the use of AI and AI agents, Cyber defenders at all levels have a monumental task to invest and continuously monitor, plan, adapt, collaborate and protect the safety of online users.

Bibliography (given sources)

GAO report to Congress

Aug 2018

Link

US Committee on Oversight and Government Reform EQUIFAX breach report

Dec 2018

Link

Appendix (additional resources)

BankInfoSecurity

Mathew J. Schwartz (euroinfosec)

May 13, 2019

Link

EPIC testimony and statement Before the House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit

Testimony and Statement for the Record of Marc Rotenberg, President, EPIC, Adjunct Professor, Georgetown University Law Center. Hearing on “Examining the Current Data Security and Breach Notification Regulatory Regime” Before the House Committee on Financial Services Subcommittee on Financial Institutions and Consumer Credit.

Feb 14, 2018

Link

Bloomberg Businessweek

By Michael Riley, Jordan Robertson, and Anita Sharpe

Sep 29, 2017

Updated on Sep 30, 2017

Link

Cybercrime Magazine
Steve Morgan, Editor-in-Chief
Sausalito, Calif. – Nov. 13, 2020
Link.

CSO Online
Josh Fruhlinger
Feb 12, 2020
Link

Senator Elizabeth Warren report
Senator Elizabeth Warren
Feb 2018
Link

Federal Bureau of Investigation
Feb 10, 2020
Link

eSafety Commissioner (Australian government)
Link

Seven Pillar Institute
Irini Kanaris Miyashiro
April 30, 2021
Link

World Economic Forum
Published Feb 19, 2025 · Updated Mar 21, 2025
Link

Act Now Stay Safe (Australian government)
Link

Google Dark Web Monitoring
Link