PROJECT REPORT – EQUIFAX

Based on the U.S. House of Representatives report on the Equifax data breach (2018)

Table of Contents

INTRODUCTION

Equifax, founded in 1899 in Atlanta, Georgia, is one of the largest consumer reporting agencies (CRAs) in the United States, maintaining credit information on over 820 million consumers and more than 91 million businesses. CRAs collect and analyze consumer data to produce credit scores and detailed reports, which they sell to third parties, including lenders and employers. Because consumers cannot opt out of this process, CRAs hold vast amounts of sensitive personal data that make them highly attractive targets for cyberattacks. This places a heightened responsibility on CRAs, such as Equifax, to apply strong security measures and to implement best-in-class data security practices to ensure the protection of consumer information.

On September 7, 2017, Equifax announced a cybersecurity incident affecting 143 million consumers, later revised to 148 million, which is nearly half of the U.S. population. The breach originated from a critical vulnerability in the Apache Struts web application framework, publicly disclosed on March 7, 2017. Despite timely alerts from the Department of Homeland Security and internal notifications from Equifax's Global Threat and Vulnerability Management (GTVM) team, the company failed to patch its Automated Consumer Interview System (ACIS)—a legacy, internet-facing portal developed in the 1970s.

Attackers exploited this vulnerability to gain access to 48 databases containing sensitive personal information, including Social Security numbers, birth dates, addresses, driver's license numbers, and, in some cases, credit card numbers. The attackers remained undetected for 76 days, highlighting significant gaps in monitoring, patch management, and overall cybersecurity governance.

This report examines the Equifax 2017 data breach by exploring the sequence of events leading to the incident, the underlying causes, organizational failures, and the consequences of the breach.

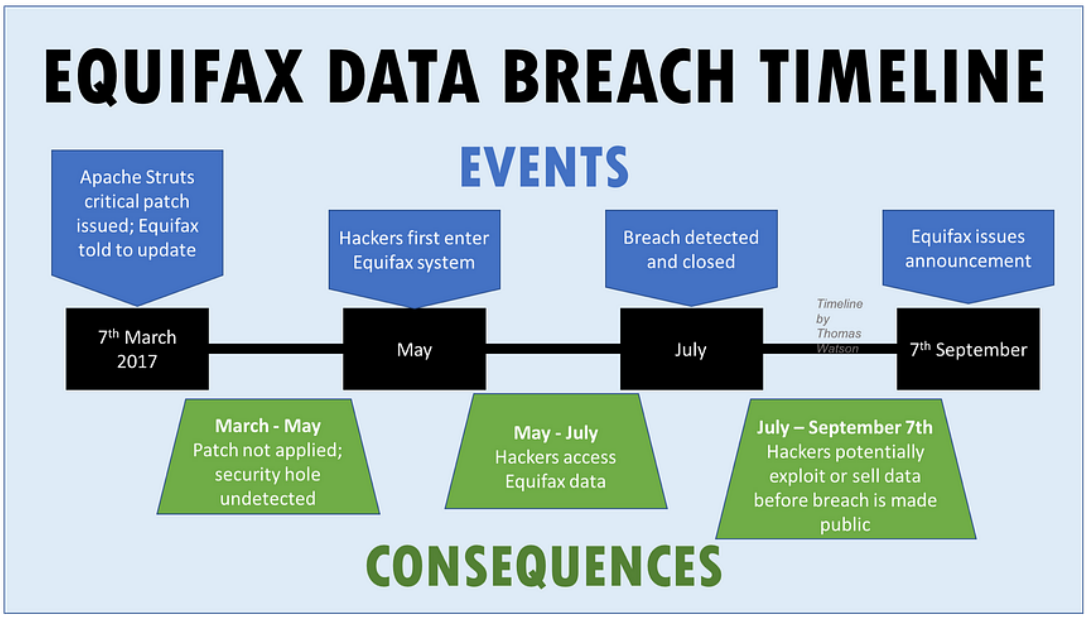

Figure 1. Equifax data breach timeline (Watson, 2017).[1]

EVENTS LEADING TO THE BREACH

The 2017 Equifax breach unfolded over several months, beginning with the disclosure of a critical vulnerability in Apache Struts and culminating in attackers gaining access to multiple sensitive databases.

1. Apache Struts Vulnerability Timeline

Apache Struts is an open-source web application framework that allows applications to run on a server's operating system. Key events with respect to the Apache Struts vulnerability are as follows:

- **February 14, 2017:** A security researcher reported a flaw in Apache Struts to the Apache Software Foundation.
- **March 7, 2017:** The Apache Struts Project Management Committee publicly disclosed the vulnerability, which allowed remote code execution via file uploads. Security experts immediately noted the potential for high impact with low complexity and added it to the National Vulnerability Database, naming it as CVE-2017-5638.
- **March 8–9, 2017:** US-CERT issued a notice to Equifax recommending immediate patching. The GTVM team and approximately 430 recipients received instructions to upgrade Apache Struts within 48 hours.
- **March 10–16, 2017:** Equifax's internal scanning tools failed to detect the vulnerable system due to misconfigurations. Meanwhile, Attackers simultaneously began network reconnaissance.

2. Initial Compromise and Attack Vector

- **May 13, 2017:** Attackers exploited the Apache Struts vulnerability in Equifax's ACIS, a legacy portal for credit dispute investigations.
- **Attack Vectors Used** -
    - **Web Shell Deployment:** Attackers uploaded multiple web shells, which allowed them to execute commands, manipulate files, and move laterally across the network.
    - **Privilege Escalation:** Unencrypted credentials stored in shared files enabled access to 48 unrelated databases.
    - **Data Exfiltration:** Attackers ran roughly 9,000 queries, extracting PII from 265 files and transferring it via Wget commands.

3. Detection and Response Initiation

- **July 29, 2017:** The Countermeasures team restored SSL traffic monitoring and detected suspicious requests from Chinese IP addresses.
- **July 30, 2017:** Vulnerability testing revealed SQL injection and Insecure Direct Object Reference flaws in ACIS. The team observed additional suspicious traffic, prompting an emergency shutdown of the ACIS portal at 12:41 pm.

- **July 30, 2017:** CSO Susan Mauldin was informed of the incident and joined an incident management conference call, marking the start of Equifax's formal response efforts.

EVENTS FOLLOWING THE BREACH

The aftermath of the breach involved a sequence of internal discovery, forensic investigation, public notification, and organizational fallout. This section outlines the timeline of events following the initial breach, from late July 2017 to early 2018, with a focus on Equifax's actions, challenges, and responses.

1. Discovery and Initial Incident Response

- **July 30, 2017:** Equifax continued its investigation into the ACIS system and discovered critical flaws in its coding. The team identified two major vulnerabilities:
  1. **SQL Injection** – This flaw allowed attackers to inject or retrieve sensitive database information without authorization.
  2. **Insecure Direct Object Reference** – This vulnerability permitted direct access to system data without proper authentication, further compromising security.

  Following these discoveries, Equifax observed additional suspicious network traffic originating from an IP address leased to a Chinese provider. In response, the company took emergency action and shut down the ACIS web portal at 12:41 pm on July 30, effectively ending the immediate cyberattack. CSO Susan Mauldin was informed promptly, initiating formal incident management calls.

- **July 31, 2017:** Equifax designated the incident response as Project Sierra. The Vulnerability Assessment team reviewed the ACIS application findings and discovered an unexpected JavaServer Pages (JSP) file inserted via SQL injection. This file effectively acted as a web shell, enabling attackers to execute arbitrary commands on the server. A second JSP file was later identified. Equifax's forensic team imaged the compromised environments immediately. A review of prior vulnerability scans revealed that a January 25, 2017, scan had detected a remediated Apache Struts vulnerability, but the ACIS application was still running a vulnerable version.

2. Forensic Investigation and Internal Coordination

- **August 2017:** Equifax engaged the cybersecurity firm Mandiant to conduct a comprehensive forensic review, beginning August 3 and continuing until October 2, 2017. Mandiant preserved databases accessed by the attackers, analyzed suspicious queries, and reconstructed the attackers' steps.

  Key milestones during this phase:

  - **August 11:** Potential access to consumer PII identified.
  - **August 15 - 17:** Leadership confirmed a significant PII compromise and coordinated with Mandiant to reconstruct the attacker

- **August 24–27:** Mandiant coordinated with Equifax database owners to confirm the exact scope of compromised data, a challenging process due to the lack of clear database ownership and inconsistent data labelling.

During this period, Equifax also briefed its Board of Directors and initiated Project Sparta, a parallel effort to prepare public notification infrastructure, including a dedicated website and call centers for consumer assistance.

3. Preparing Public Notification

- **Project Sparta:** In mid-August 2017, Equifax launched Project Sparta to provide consumers with access to breach information, credit monitoring, and identity protection services. A dedicated website, equifaxsecurity2017.com, was developed to inform individuals of their exposure and facilitate enrolment in protective services.
- **Challenges:**
  - Website overload due to high traffic
  - Perceived security issues and phishing risks
  - Call center staffing shortages are causing delays and consumer frustration.

4. Public Announcement and Immediate Fallout

- **September 7, 2017:** Equifax publicly announced the breach. Exposed data included names, Social Security numbers, birth dates, addresses, driver's license numbers, credit card numbers, and credit dispute documents.
- **Leadership changes**: CIO David Webb and CSO Susan Mauldin retired on September 15, and CEO Richard Smith resigned on September 26.

5. Completion of Forensic Investigation and Employee Termination

- **October 2, 2017:** Mandiant concluded the forensic review, identifying an additional 2.5 million affected consumers. Hidden database queries via web shells were uncovered, which were created by the attackers.
- **Termination of Graeme Payne:** Graeme Payne, Senior VP and CIO for Global Corporate Platforms, was terminated for failing to forward the March 9 Apache Struts patch alert. Payne was one of 430 employees copied on the alert, and he testified that he had no directive to forward it.

The complexity of Equifax's IT environment, including unclear database ownership, multiple data tables, and legacy systems, made forensic analysis a meticulous and time-consuming process, requiring several weeks to establish an accurate count of affected individuals.

CAUSE OF THE BREACH

The 2017 Equifax breach resulted from a combination of technical vulnerabilities, operational gaps, and systemic weaknesses in governance. While the immediate trigger was the exploitation of a publicly known Apache Struts vulnerability (CVE-2017-5638), the underlying causes reveal broader organizational failings that allowed attackers to gain prolonged, undetected access to sensitive consumer data. A comparison with the 2018 JPL/NASA breach highlights that such failures are not unique to private enterprise: legacy systems, unclear accountability, and delayed updates create vulnerabilities across organizations, whether safeguarding consumer financial data or mission-critical research systems.

1. Exploitation of a Known Vulnerability

The attackers gained entry through a critical vulnerability in the Apache Struts web application framework. This vulnerability allowed unauthenticated remote code execution on Equifax's internet-facing web application, the ACIS. Although a patch was publicly released on March 7, 2017, and alerts were sent internally, Equifax failed to apply it to the ACIS servers. This gap created a direct path for attackers to inject malicious code and establish persistent access. The unpatched system demonstrates that security alerts alone are insufficient without clear ownership and follow-through—the expired SSL certificate, for example, was not just a technical oversight; it reflected systemic governance failure, as no one owned certificate management.

Similarly, in the JPL incident, outdated credentials in legacy NASA systems remained exposed for months due to delayed patching and inconsistent oversight. Both cases underscore that alerts alone are insufficient without clear ownership and follow-through.

2. Delayed Patch Management and Operational Gaps

Equifax lacked consistent, enforceable processes for patching critical vulnerabilities. High-priority patches were not deployed within the recommended 48-hour window due to unclear accountability, reliance on manual processes, and limited automation for tracking compliance. Operational gaps extended beyond patching: monitoring tools were poorly maintained, and unusual activity went undetected for months. The JPL case mirrored these delays, demonstrating how gaps in routine updates and audits prolong exposure windows and amplify risk.

3. Blind Spots in Security Monitoring

Even after attackers gained access, ongoing exfiltration of sensitive data went undetected for months. A key factor was that the network monitoring tool, which should have flagged unusual activity, relied on an expired digital certificate. This certificate had expired for nearly 19 months, effectively blinding

the monitoring system to abnormal data flows. This lack of visibility demonstrates a deeper organizational failure, where monitoring tools existed but were not actively managed.

In JPL's incident, monitoring gaps in legacy mission systems were identified post-incident, highlighting that even critical government systems can have delayed detection capabilities when older infrastructure and manual oversight intersect.

4. Legacy Systems and Complex Infrastructure

Equifax's IT environment was highly fragmented, with critical systems running on legacy platforms that lacked proper segmentation. Rapid acquisitions under CEO Richard Smith added complexity, integrating diverse systems without standardized security practices. Poor inventory management and undocumented interdependencies further hindered visibility and containment. NASA's JPL environment shared similar challenges: mission-critical legacy systems, weak documentation, and inadequate integration created operational blind spots that attackers could exploit.

5. Weak Access Controls and Privilege Management

Attackers exploited overly broad administrative privileges, allowing access across multiple systems. Weak role-based access controls and limited monitoring of privileged activity amplified the scale of the breach, exposing PII for over 145 million consumers.

6. Lack of Accountability and Role Clarity

Interviews and internal investigations revealed unclear responsibility for critical security functions. Many employees in transcribed interviews admitted that they did not know who owned patch management, monitoring, or vulnerability response tasks. This demonstrates a systemic governance failure, where technical flaws intersect with organizational weaknesses.

7. Systemic Organizational Failures

Beyond technical vulnerabilities, these governance issues contributed directly to the breach. There was a persistent gap between corporate security policies and operational execution, and failure to define accountability created blind spots that attackers exploited. Vulnerability alerts, monitoring failures, and patching gaps were not escalated effectively to leadership. Similarly, the JPL breach exposed lapses in policy enforcement, where unauthorized devices and weak network controls persisted despite formal security guidelines.

RESULT OF THE BREACH

1. Business and Organizational Impact

- **Reputation and Public Trust:** The breach affected approximately 148 million U.S. consumers, nearly half of the population. Equifax faced widespread criticism for delayed notifications and inadequate consumer support. Its dedicated breach website and call centers were overwhelmed, compounding public frustration.
- **Financial Consequences:** Equifax's stock fell 35% in the first week post-disclosure, erasing $6 billion in market value. While 2017 revenue grew to $3.362 billion, incident-related costs for the first nine months of 2018 reached $221.5 million. Legal settlements and regulatory penalties have exceeded $575 million.
- **Leadership Changes and Oversight:** The breach prompted rapid executive turnover: CIO David Webb and CSO Susan Mauldin retired in September 2017, followed by CEO Richard Smith. Regulatory scrutiny intensified, with investigations launched by the FTC and CFPB, and multiple Congressional hearings convened.
- **Long-Term Consequences:** Beyond immediate costs, Equifax faced loss of business contracts, mandated ongoing audits, and persistent regulatory oversight.

2. Technical and Data Impact

- **Scope of Data Compromised:** Attackers accessed PII for 148 million individuals, including names, Social Security numbers, birth dates, addresses, and driver's license information. Additionally, 209,000 credit card numbers and credit dispute documents for 182,000 consumers were compromised. The attackers queried 48 unrelated databases, conducting roughly 9,000 queries, with 265 queries successfully returning unencrypted PII datasets. None of the affected PII was encrypted at rest.
- **Attack Methodology and System Weaknesses:** Attackers exploited the Apache Struts vulnerability (CVE-2017-5638), installed approximately 30 web shells, and moved laterally through inadequately segmented networks. The breach remained undetected for 76 days, partly due to an expired SSL certificate used for monitoring ACIS network traffic and a lack of robust logging and access controls.
- **Challenges for Forensic Investigation:** Inconsistent database labeling, absence of system ownership, and a fragmented legacy IT environment complicated incident response, delaying accurate assessment of the breach's full scope.

FAILURES AND HOW THEY COULD HAVE BEEN AVOIDED

Finding	How It Could Have Been Avoided
Lack of centralized accountability in IT and security leadership	Implement clear reporting structures between IT, security, and executive management. Assign ownership of critical functions (patching, monitoring, vulnerability management) to named

	roles with executive oversight. Regularly review responsibility assignments to ensure accountability.
Inadequate patch management and delayed response to known vulnerabilities	Establish automated, proactive vulnerability scanning and patch deployment systems. Critical vulnerabilities should be patched within 48 hours, following benchmarks from enterprise security standards (e.g., NIST SP 800-40) [2]. Escalate high-risk alerts to leadership immediately.
Failure to maintain an accurate inventory of IT assets and software	Maintain a unified, continuously updated asset registry, including legacy systems. Implement automated discovery tools to track software versions, system dependencies, and end-of-life components.
No enforced network segmentation between critical systems	Design systems with network segmentation and restrict internal access to sensitive databases, limiting lateral movement in case of breach.
Absence of file integrity monitoring on legacy applications	Deploy file integrity monitoring (FIM) tools across all mission-critical systems, including legacy applications. Configure automated alerts and enforce immediate investigation of unauthorized changes.
Poor SSL certificate management led to blind spots in encrypted network monitoring.	Implement automated SSL/TLS certificate management (e.g., using services like Let's Encrypt or enterprise PKI tools). Perform quarterly audits to ensure all certificates are valid and correctly configured [3].
Insufficient logging and short log retention disabled incident reconstruction	Configure centralized log aggregation with retention periods aligned to regulatory requirements. Ensure logs include critical events (authentication, configuration changes, privileged access, etc.) for forensic readiness.
Expired and incomplete operational policies ("honor system" for patching)	Formalize policies with documented compliance checks. Require periodic audits and executive sign-off to enforce adherence. Tie performance metrics to policy compliance.
Legacy IT infrastructure that was complex and difficult to secure	Accelerate modernization initiatives: migrate critical applications off legacy systems, retire obsolete technology,

	and standardize platforms. Prioritize high-risk systems for immediate upgrade.
Slow organizational adaptation after warnings and audits	Implement structured remediation tracking after audits or penetration tests. Report progress directly to executive leadership and governing boards. Set measurable deadlines and consequences for missed actions.
Lack of modern monitoring and response (SIEM/SOAR)	Deploy SIEM for real-time log correlation and threat detection. Layer SOAR for automated incident response, playbooks, and containment. Benchmark monitoring effectiveness against industry standards (e.g., MITRE ATT&CK, Gartner Magic Quadrant) [4]

SIEM vs SOAR

A Security Information and Event Management (SIEM) system aggregates and correlates logs to identify suspicious activity. In Equifax's case, a functioning SIEM with active SSL inspection could have flagged the abnormal queries and traffic exfiltration months earlier.

A Security Orchestration, Automation, and Response (SOAR) platform extends SIEM by automating incident-handling. For example, once anomalous database queries were detected, SOAR could have automatically quarantined affected servers, blocked malicious IPs, or escalated alerts without delay.

Equifax's failure illustrates both a detection gap (no SIEM visibility due to expired certificates) and a response gap (manual, slow containment). Modern enterprises rely on SIEM for visibility and SOAR for speed — both of which were missing here.

THIRD PARTY ANALYSIS – FINDINGS AND RECOMMENDATIONS

The Equifax breach triggered widespread scrutiny from government agencies, consulting firms, privacy advocates, and technical analysts. Each lens highlights a different aspect of the failure, revealing that the breach was not only a technical incident but also a failure of corporate governance, regulatory oversight, and consumer protection frameworks.

1. U.S. Government Accountability Office (GAO, 2018) [5] - *Government Perspective*

The GAO framed Equifax as a systemic risk, given that CRAs hold financial data on nearly every adult American. The report emphasized that inadequate oversight of CRAs poses a national security and economic threat.

Key findings:

- Failures in patch management, network segmentation, and monitoring.
- Lack of government oversight over private credit bureaus.

Recommendations:

- Implement stronger federal standards for safeguarding consumer data.
- Increase CRA accountability in handling sensitive financial information.
- Improve oversight of federal agencies that rely on CRA data.

2. Oliver Wyman / Marsh [6] - *Enterprise Risk Management Perspective*

Oliver Wyman and Marsh analyzed Equifax as an enterprise risk failure. They argued that cybersecurity should be treated as a core business risk, not solely a technical one.

Key findings:

- Equifax underestimated the scale of cyber risk exposure.
- Breach risk modeling was insufficient compared to natural disasters or financial crises.

Recommendations:

- Integrate cyber risk into ERM frameworks and board-level risk discussions.
- Align cyber insurance and financial reserves with actual exposure.
- Treat cybersecurity as a strategic business concern, not just an IT issue.

3. Office of the Privacy Commissioner of Canada (OPC, 2019) [7] - *Privacy Oversight*

The OPC examined Equifax Canada's handling of Canadians' personal information and found violations under PIPEDA. (Canada's privacy law).

Key findings:

- Cross-border data transfer risks: Canadian data stored on U.S. servers lacked equivalent protections.
- Poor oversight of subsidiaries by the U.S. parent.

Recommendations:

- Strengthen governance of Canadian operations and third-party processors.
- Improve cross-border safeguards for personal data.

4. Electronic Privacy Information Center (EPIC) [8] - *Consumer Advocacy*

EPIC highlighted delayed notifications, limited remedies, and the broader issue of consumer rights when CRAs operate with minimal regulation. Their recommendations included:

Key findings:

- Consumers cannot opt out of CRA databases.
- Remedies offered post-breach were inadequate.

Recommendations:

- Limit retention of unnecessary sensitive data.
- Establish statutory liability for failures to protect personal information.
- Expand consumer rights to control data usage.

5. Breachsense, Technical Case Study (2024) [9] - *Technical Perspective*

Breachsense provided a technical retrospective, emphasizing operational lessons and preventable errors.

Key findings:

- Breach could have been prevented with faster patching and automated certificate management.
- Lack of zero-trust segmentation and insufficient log retention allowed attackers to move freely and avoid detection.
- Weak cybersecurity measures contributed to geopolitical risks, connecting to later U.S. indictments of Chinese military hackers.

Recommendations:

- Apply automated patching and certificate renewal processes.
- Deploy zero-trust network segmentation.
- Retain logs long enough for forensic analysis.

REFERENCES

[1] Watson, T. (2017, September 15). *How Equifax royally screwed up – unravelling the biggest hack of 2017 (or ever?)* Medium. https://medium.com/@thomaswatson_3014/how-equifax-royally-screwed-up-unravelling-the-biggest-hack-of-2017-or-ever-4511b12a3e1b

[2] National Institute of Standards and Technology. (2013). *Guide to enterprise patch management planning: Recommendations of the National Institute of Standards and Technology* (NIST Special Publication 800-40 Rev. 4). https://csrc.nist.gov/pubs/sp/800/40/r4/final

[3] Let's Encrypt. (n.d.). *Certificate management best practices*. Retrieved September 13, 2025, from https://letsencrypt.org/docs/

[4] Gartner. (2024). *Magic Quadrant for security information and event management*. Gartner. Retrieved September 13, 2025, from https://www.gartner.com/reviews/market/security-information-event-management

[5] U.S. Government Accountability Office. (2018, August 30). *Data protection: Actions taken by Equifax and federal agencies in response to the 2017 breach* (GAO-18-559). Retrieved from https://www.gao.gov/assets/gao-18-559.pdf

[6] Mee, P., & DeBrusk, C. (2017, September). *The Equifax data breach and its impact on identity verification*. Oliver Wyman & Marsh. Retrieved from https://www.marsh.com/content/dam/oliver-wyman/v2/publications/2017/sep/Oliver_Wyman_Equifax_Data_Breach.pdf

[7] Office of the Privacy Commissioner of Canada. (2019, April 9). *PIPEDA findings #2019-001: Investigation into Equifax Inc. and Equifax Canada Co.'s compliance with PIPEDA in light of the 2017 breach*. Retrieved from https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2019/pipeda-2019-001/

[8] Electronic Privacy Information Center. (2017, September 8). *143 million U.S. consumers suffer massive data breach at Equifax*. Retrieved from https://archive.epic.org/privacy/data-breach/equifax/

[9] Breachsense. (2024, August 14). *Equifax data breach: A technical retrospective*. Retrieved from https://www.breachsense.com/blog/equifax-data-breach/