CAPSTONE POINT PAPER
Title: Case Study Point Paper – Equifax Data Breach, 2017
Date: April 24, 2025
Author: Subhadra Mahanta

Case Study Point Paper – Equifax Data Breach

I. Overview:

Breach:

- On *March 6th 2017*, Apache publicly announced **CVE-2017-5638**, a critical OGNL (a type of flaw allowing arbitrary code to run through manipulated HTTP headers) injection flaw in the Struts 2 web framework along with the fix.
- Equifax, a credit titan, left every vulnerable system unpatched.
- Starting *May 12th 2017*, 2 months after the vulnerability announcement, attackers exploited the vulnerability to Deploy web shells to access Equifax's data servers, granting *unauthorised access to nearly 44% of the US population's critical data*.
- Over the next 10 weeks, data was pulled out of the network in encryption form, undetected by Equifax's monitoring systems.
- *July 29th 2017*, Equifax discovered that a breach had taken place and tens of millions of critical consumer data was compromised.
- *September 7th 2017*, 6 weeks after the breach discovery, Equifax publicly announced the breach.

Scope:

- 147.9 million US citizens, 15.2 million British citizens and about 19 thousand Canadian citizen's sensitive information was compromised, including social security numbers, date of birth, etc.
- 209 thousand US credit card numbers were stolen
- More than 30 lawsuits were filed against Equifax
- Several high-ranking executives were accused of corruption
- Following the breach, Equifax's CEO, CIO and CSO resigned.
- Equifax's stock dropped by 13%
- Equifax had to pay over 700 million dollars in settlement.

II. Organizational and Governance Failures:

- **Poor Patch Management**: No enforcement or follow-up mechanism for critical patches.
- **Poor Asset Management and Risk-Based Prioritization**: Poor asset management, no prioritization, no accountability.
- **IAM Failures**: No enforcement of strong credential policies.

- **Inadequate Monitoring and Detection**: No processes for ensuring critical certificates are renewed.
- **Poor Network Segmentation**: Lack of internal controls and network segmentation.
- **Delayed Disclosure and Public Transparency**: Delayed disclosure + executives sold stocks right before disclosure; raising questions about the ethics, compliance and insider trading from the executives.
- **Inadequate Oversight from Board and Executives**: Security wasn't treated as board-level concern.

III. Major Root Cause:

Root Cause: A broken vulnerability management system. Critical patch notifications went ignored, and no one was held accountable.

Immediate Exploitable Weakness: Internet-facing Struts modules were running on unpatched code. Attackers utilised the HTTP headers to send malicious code (the vulnerability allowed execution while checking the files) for remote code execution.

Systemic Failures:

- ▪ **Flat Network Architecture:** No barriers once attackers were in.
- ▪ **Lack of Data Encryption at Rest:** PII stored in plaintext or with weak, reversible encryption made exfiltration very easy.
- ▪ **Weak Identity and Access Management (IAM):** Service accounts with broad privileges and no multi-factor authentication (MFA) amplified blast radius once inside.

IV. Equifax's Missteps in Incident Response:

- **Detection vs. Disclosure Lag:** The eight-week gap between July detection and September disclosure, stands against GDPR's current mandatory notification period – within 72 hours.
- **Delayed Credential Revocation:** Even after identifying malicious web shells, service and administrative credentials remained active for days, enabling repeat unauthorised access.
- **Faulty Communications:** Public FAQs went live only after massive customer backlash, contradictory messaging deepened distrust. A compromised 'help' website even inadvertently exposed further technical details.
- **Inadequate Forensic Scope:** Internal forensics initially focused on web servers, ignoring unmonitored backups and archived logs that attackers later abused to re-access.

- **Executive Inaction:** The CEO and CSO delayed taking responsibility. The CEO spoke to Congress just 19 days before resigning, showing a slow, reactive response.

V. Alternative Incident Response Strategy by me:

- **Patch Verification Protocol:** Enforce a zero-tolerance policy for unpatched high-severity CVEs. Every critical patch gets a follow-up audit.
- **Early Detection Systems:** Deploy real-time threat detection tools across web-facing assets, including Monitoring Log files and enforcing Anomaly detection systems, Intrusion Detection Systems and Intrusion Prevention Systems.
- **Playbook-Based Response:** Prepare breach-specific incident response playbooks, including communication strategy, legal engagement and third-party notification timelines.
- **Red Team Exercises:** Have regular Red Team Exercises as well as adequate compensation for external vulnerability reporting.

VI. Suggested Preventive and Mitigative Steps:

- **Implement the NIST Cybersecurity Framework (CSF) thoroughly:** Especially in Identify, Protect, Detect and Response strategies. Equifax failed in all four of them!
- **Zero Trust Architecture:** Implement Zero trust architecture including network segmentation with individual firewalls, IDS/IPS, etc.; Implement reauthentication and reauthorization for both lateral and vertical movement within the network.
- **Software Bill of Materials**: Integrate SBOM for dependency visibility.
- **Automated Attack Surface Monitoring:** Utilise advance attack surface monitoring systems to detect zero-day vulnerabilities.
- **AI-assisted anomaly detection** to flag unexpected data access behaviour in real time
- **Regular Security Audits:** Have regular independent security audits.
- **Full Encryption:** Have both data at rest and in transit be within encryption.
- **Employee Training and Accountability:** Regular Employee Training and Accountability builds robust security culture within an organisation.

VII. Key Lessons and Takeaways:

- **Clear Responsibility**: Every known software bug (CVE) should have someone clearly responsible for fixing it. Set deadlines to fix them and report delays to higher-ups.

- **Be Proactive over Reactive**: Don't wait until a breach happens. Embed security into the software development process from the start. Assume we are breached and actively hunt for clues – Threat Hunting.
- **Zero Trust Policy**: Split the network into secure parts, encrypt all data, and make sure every system, inside or outside, has to prove who it is before connecting.
- **Security Drills**: Keep watching for threats constantly. Also run monitored red team drills and fix security gaps while the drill is still happening, not after it's over (get used to playbooks).
- **Transparency**: If there's a breach, tell the public and regulators honestly and quickly. Being open builds trust and can reduce future fines and lawsuits.

The Equifax breach resulted in the loss of not only data but also trust, market value, and leadership credibility. This wasn't just a breach, but a case study on **what not to do**!

VIII. Sources:

- https://en.wikipedia.org/wiki/2017_Equifax_data_breach#:~:text=On%20September%2026%20Equifax%20announced,Paulino%20do%20Rego%20Barros%20Jr.

- https://sevenpillarsinstitute.org/case-study-equifax-data-breach/#:~:text=On%20July%2029th%2C%20Equifax%20renewed,collect%20American%20data%20(Fruhlinger).

- https://www.youtube.com/watch?v=_6Qbslgpw8U&t=206s

- https://www.youtube.com/watch?v=g6sb6LhO0U4

- https://www.cnbc.com/2019/02/13/equifax-mystery-where-is-the-data.html

- https://www.secureworld.io/industry-news/equifax-breach-social-media

- https://www.cnbc.com/2018/03/14/former-equifax-executive-charged-with-insider-trading-ahead-of-data-breach.html

- https://www.secureworld.io/industry-news/equifax-post-breach-why-the-ceo-survived-just-19-days

CAPSTONE POINT PAPER
Title: Case Study Point Paper – Equifax Data Breach, 2017
Date: April 24, 2025
Author: Subhadra Mahanta

- https://www.secureworld.io/industry-news/day-by-day-timeline-of-equifax-breach

- https://www.youtube.com/watch?v=bh1gzJFVFLc