Equifax Case Study

Date: 2024-11-15

Handler: Chao Tang

1. Introduction

The 2017 Equifax data breach, which exposed sensitive personal information of 147.9 million individuals, serves as a landmark case study in cybersecurity failures. Rooted in a failure to patch a known vulnerability in Apache Struts, the breach revealed systemic weaknesses in Equifax's cybersecurity practices: delays in detection and response, combined with insufficient network segmentation and weak data governance, allowed attackers to exploit vulnerabilities and remain undetected for over 2 months. This breach resulted in massive financial, legal, and reputational damage, culminating in a $700 million settlement. By examining Equifax's failures and comparing them to other breaches, such as NASA's, the case highlights the critical need for robust security measures, proactive governance, and a culture of prioritizing data protection.

2. Difference Between SIEM and SOAR

SIEM (Security Information and Event Management) systems focus on collecting, analyzing, and correlating log and event data from across an organization's IT infrastructure. They provide centralized visibility into potential threats by aggregating data from various sources, such as firewalls, servers, and endpoint devices. SIEM tools excel at:identifying anomalies or suspicious patterns in real-time and generating alerts, providing historical data and context to investigate incidents after detection, and assisting organizations in meeting regulatory requirements by maintaining and analyzing log data. SIEM for short, is a solution that helps organizations detect, analyze, and respond to security threats before they harm business operations.

SOAR (Security Orchestration, Automation, and Response) platforms extend beyond detection by automating and orchestrating the response to security threats. They integrate various security tools and workflows, enabling organizations to: automating

routine repetitive processes like phishing analysis or malware triage without human intervention, coordinating actions across tools (e.g., firewalls, endpoint protection) to respond to threats, providing a unified dashboard for managing incidents and streamlining workflow, and enabling better communication among teams with clear playbooks and automated processes.

3. Events Leading to the Breach

CVE-2017-5638 was a remote code execution vulnerability in Apache Struts. This flaw allowed attackers to manipulate file upload params to enable paths traversal via the Jakarta Multipart parser and, under some circumstances, this can lead to uploading a malicious file which can be used to perform remote code execution. Specifically, attackers could send specially crafted HTTP headers to the vulnerable server, which would process them and execute malicious commands on a server.

Although this vulnerability was disclosed in March 2017, along with available patches, Equifax did not apply the update to their systems. This oversight allowed attackers to exploit the unpatched system and gain unauthorized access. Sensitive data, including personally identifiable information, was stored without adequate segmentation. Attackers conducted thorough reconnaissance to map Equifax's network and identified valuable data repositories, and accessed them across multiple databases once they breached the initial system without triggering alarms, as there were no barriers preventing lateral movement within the network. There was also a significant disorganization of leadership and oversight regarding Equifax’s cybersecurity policies and practices, exacerbating the systemic failures.

Despite the breach commencing in mid-May 2017, Equifax's security logging and monitoring systems failed to detect the unauthorized access for over 76 days, until July 29, 2017. This prolonged undetected period allowed attackers to steal vast amounts of personal information without interruption. The delay in detection was partly due to an expired Secure Sockets Layer (SSL) certificate on a network monitoring device, which had lapsed for 19 months. Once renewed, the device immediately flagged suspicious traffic, indicating that the failure of timely maintenance of security tools would lead to catastrophic consequences in threat detection.

4. Events Following the Breach

After the expired SSL certificate was renewed, Equifax's Countermeasures team began inspecting network traffic. They detected a suspicious request originating from a Chinese IP address. Using the tool Moloch, an open-source software for analyzing packet captures, the team identified persistent attempts to contact the ACIS web portal. Suspicious packets, each containing more than 10 MB of headers and payloads possibly related to credit investigations, were flagged for further analysis. On July 30, 2017, Equifax conducted vulnerability testing on the ACIS application and discovered flaws like SQL injection and Insecure Direct Object Reference attacks, which enabled unauthorized access to sensitive data. Equifax then shut down the ACIS web portal for emergency maintenance, and blocked the suspicious Chinese IP address and its associated ISP.

Forensic investigations were then conducted. It revealed unexpected JSP (JavaServer Pages) files in the ACIS environment, which attackers used to create web shells. These shells allowed remote command execution on compromised servers. Vulnerability assessments conducted on July 31, 2017, confirmed that a version of Apache Struts vulnerable to CVE-2017-5638 was still in use, contradicting earlier scans from April 2017 that found no un-remediated vulnerabilities. Also on July 31, 2017, Equifax's forensic team concluded that personally identifiable information (PII) was likely exfiltrated. However, there was no complete understanding of the scale of the breach or the specific data compromised at that time.

Senior leadership, including the Chief Security Officer, informed key personnel of the incident. However, communication gaps persisted: the CSO failed to notify the Chief Information Officer of potential PII exfiltration until weeks later; the Chief Legal Officer was informed but did not respond immediately. On August 1, 2017, investigations continued under the project codename Project Sierra. The team discovered further evidence of unauthorized data access and exploitation of Apache Struts vulnerabilities. On August 3, 2017**,** an SSL certificate was finally loaded onto a secondary server used by ACIS, improving visibility into traffic. However, the delay prevented a full understanding of earlier activity. On September 7, 2017, Equifax eventually discovered the full scope of the breach: sensitive information of 147.9 million individuals, including Social Security numbers, birth dates, and credit information, was stolen.

5. Cause and Result of the Breach

Cause:

The primary cause was the exploitation of the CVE-2017-5638 vulnerability in Apache Struts. Despite a patch being released in March 2017, Equifax failed to update its

systems in time. Moreover, inadequate Incident Response protocols and systemic security weaknesses contributed to the breach.

Result:

1. Personal data of 147.9 million individuals was stolen, including Social Security numbers, birth dates, and credit information.
2. Equifax faced lawsuits and regulatory fines, leading to settlements totaling up to $700 million. The settlement included funds for affected consumers, fines for regulatory violations, and investments in improving cybersecurity.
3. The breach eroded public trust in Equifax's ability to safeguard sensitive data. Equifax's brand reputation was severely damaged.
4. Equifax became a target of investigations by multiple agencies, including the Federal Trade Commission (FTC), the Consumer Financial Protection Bureau (CFPB), and state governments. The breach set a precedent for stricter data protection laws and enforcement.
5. The breach raised global awareness about the critical importance of cybersecurity governance. It emphasized the need for proactive measures, including vulnerability management, robust incident response protocols, and better data protection practices.

6. Failures of Equifax

1. Poor patch management process. Equifax failed to implement a systematic and proactive approach to apply security patches. Despite the critical CVE-2017-5638 vulnerability being disclosed and patched in March 2017, Equifax left their systems unpatched for months, allowing attackers to exploit the flaw.
2. Inadequate network segmentation. Sensitive data was not properly segmented within Equifax's systems. This oversight allowed attackers to move laterally across the network after initial access, gaining unauthorized access to vast stores of sensitive personal information.
3. Poor communication and IR coordination. There was a lack of clear communication and coordination among internal teams during the breach response. The expired SSL certificate hindered initial detection of suspicious activity, and key information regarding the breach was not promptly escalated to leadership.
4. Weak accountability at leadership levels. Equifax's leadership failed to prioritize cybersecurity at an organizational level. Weak governance, delayed responses, and inadequate oversight of security practices exacerbated the breach's impact.

7. How Could These Failures Have Been Avoided

A structured and proactive approach to patch management could have mitigated the Apache Struts vulnerability before attackers could exploit it. Automating patch deployment and prioritizing critical updates based on their severity would ensure vulnerabilities are addressed in a timely manner. Conducting frequent penetration tests and vulnerability scans could have identified flaws like the Apache Struts vulnerability and SQL injection weaknesses before they were exploited. Using third-party cybersecurity experts for assessments would provide an additional layer of scrutiny, ensuring that blind spots in internal security processes are addressed.

Additionally, regular cybersecurity training and scenario-based training sessions for employees, especially IT and development teams, would enhance potential threats detection and awareness of best practices like patching vulnerabilities promptly. Equifax could have invested in a robust Security Information and Event Management (SIEM) system to analyze and detect anomalies in real-time. And by integrating SOAR, the company could have automated responses to detected threats, reducing the time attackers had to exfiltrate data.

One of Equifax's biggest oblivions is its reliance on outdated systems and legacy applications — technical debts. It could have modernized and secured its IT infrastructure consistently, including retiring or updating legacy systems, to reduce the attack surface. By allocating financial and human resources for technical debts, Equifax would improve overall enterprise system resilience and reduce the likelihood of unpatched vulnerabilities.

8. Comparison With the NASA Breach

In terms of insufficient security controls, NASA's Jet Propulsion Laboratory (JPL) lacked a complete and accurate inventory of its systems. The Information Technology Security Database (ITSDB) had missing and outdated entries, leading to blind spots in asset management. Weak security controls over asset registration and database updates further exacerbate the problem. The Equifax breach stemmed from the exploitation of a known vulnerability in Apache Struts due to a lack of proactive patch management. The breach detection is delayed by the absence of robust monitoring tools.

In terms of inadequate network segmentation, both organizations failed to isolate critical systems from external access. JPL’s network gateway allowed external users (e.g.,

foreign agencies, contractors, universities) to access its network remotely without proper segmentation or restrictions. External users could move laterally across the network due to a lack of isolation between internal and external-facing systems, exposing sensitive mission data. NASA also failed to establish Interconnection Security Agreements (ISA) with partner institutions to define roles, responsibilities, and security controls. Similarly, Equifax possesses poor segmentation of internal systems, which allows attackers to access sensitive data repositories without significant barriers. Once inside the network, attackers could move laterally and exfiltrate large volumes of data over 76 days.

In terms of delayed detection of breaches, slow patch management, and waiver processes, NASA's Security Problem Log tickets revealed significant delays in resolving vulnerabilities: over 5,400 unresolved tickets were found, 86% of which were labeled as high or critical severity. Patching delays were systemic, with 150 open waivers allowing issues to go unaddressed for years (some waivers were open for 7 to 10 years). NASA's ineffective waiver process permitted unresolved vulnerabilities to persist under the guise of "exceptions," creating exploitable gaps in security.

9. Third-Party Analyses of the Equifax Breach

One of the most glaring issues identified was Equifax's ineffective incident response preparation. Despite being a major repository of sensitive consumer data, Equifax lacked a robust plan for responding to security incidents. Critical monitoring tools are ineffective, leaving the company blind to ongoing suspicious activities. Cybersecurity experts argue that a well-prepared incident response team with modern tools and regular training could have significantly reduced the breach's impact by detecting and mitigating the threat earlier.

Another major criticism from cybersecurity experts was Equifax's over-reliance on outdated systems and inadequate patch management. Equifax failed to apply the CVE-2017-5638 vulnerability promptly, leaving their systems exposed for months. Third-party assessments highlighted this failure as emblematic of broader issues within the company's IT governance. Legacy systems that were not regularly updated created an expansive attack surface. Analysts suggest that timely patching and regular assessments of system vulnerabilities could have prevented the attack entirely.

Moreover, Equifax failed to prioritize cybersecurity at an organizational level. Cybersecurity experts have criticized the company's leadership for its lack of accountability and for fostering a culture where security was not treated as a strategic priority. This failure was evident in the absence of proactive measures to secure critical

infrastructure, as well as in the delayed and poorly managed public response to the breach. The combination of these factors has been cited as a cautionary example for other organizations, emphasizing the importance of strong leadership and corporate policies that embed cybersecurity into all aspects of operations.