

|  |
| --- |
| * Introduction * Background * Branch Details * Impact * Response * Leason Learned * Conclusion * Reference   TABLE OF CONTENT  Cybersecurity Breach Report:  The Equifax Breach (2017) **Prepared by:** Madhumitha B. **Institution:** Velammal Engineering College, Department of AI & DS **Date:** October 2024 **INTERN COMPANY NAME:** NULL CLASS  (TASK 2 REPORT) |
| Page 1 |

|  |  |  |
| --- | --- | --- |
| INTRODUCTION | | * The Equifax data breach, one of the most significant cybersecurity incidents in recent history, affected over 147 million consumers. * The breach, which occurred in 2017, exposed sensitive personal information such as Social Security numbers, birth dates, and addresses. * This report analyzes the breach by examining its background, how it occurred, its impact, the response by Equifax, and the lessons learned. |
| BRANCH DETAILS  BACKGROUND | TIME LINE OF BREACH HOW IT OCCURRED, VULNERABILITIES AND METHOD USED :  * The breach occurred between May and July 2017 but wasn’t disclosed to the public until September 2017. * Attackers exploited a vulnerability in the Apache Struts web application framework used by Equifax. Despite the availability of a patch in March 2017, Equifax failed to apply it promptly * The vulnerability (CVE-2017-5638) allowed attackers to execute arbitrary code on the web server. * Failure to update the software exposed the system to attack.  “HISTORY AND CONTEXT OF EQUIFAX”  * Equifax is a global consumer credit reporting agency, one of the three largest in the U.S., along with Experian and TransUnion. * Established in 1899, Equifax provides credit information to businesses to assist in credit decisions. * Given its core function, the company stores massive amounts of sensitive personal data, making it a high-value target for cybercriminals. * By 2017, Equifax had expanded globally, managing credit data for millions of consumers, emphasizing the critical nature of its data security. | |

* The vulnerability (CVE-2017-5638) allowed attackers to execute arbitrary code on the web server.
* Failure to update the software exposed the system to attack.
* Attackers infiltrated Equifax's system using an SQL injection attack.
* Once inside, they gained access to a wide range of sensitive information over several months before being detected.
* Poor segmentation of Equifax’s internal systems allowed hackers to move laterally and access vast amounts of personal data.

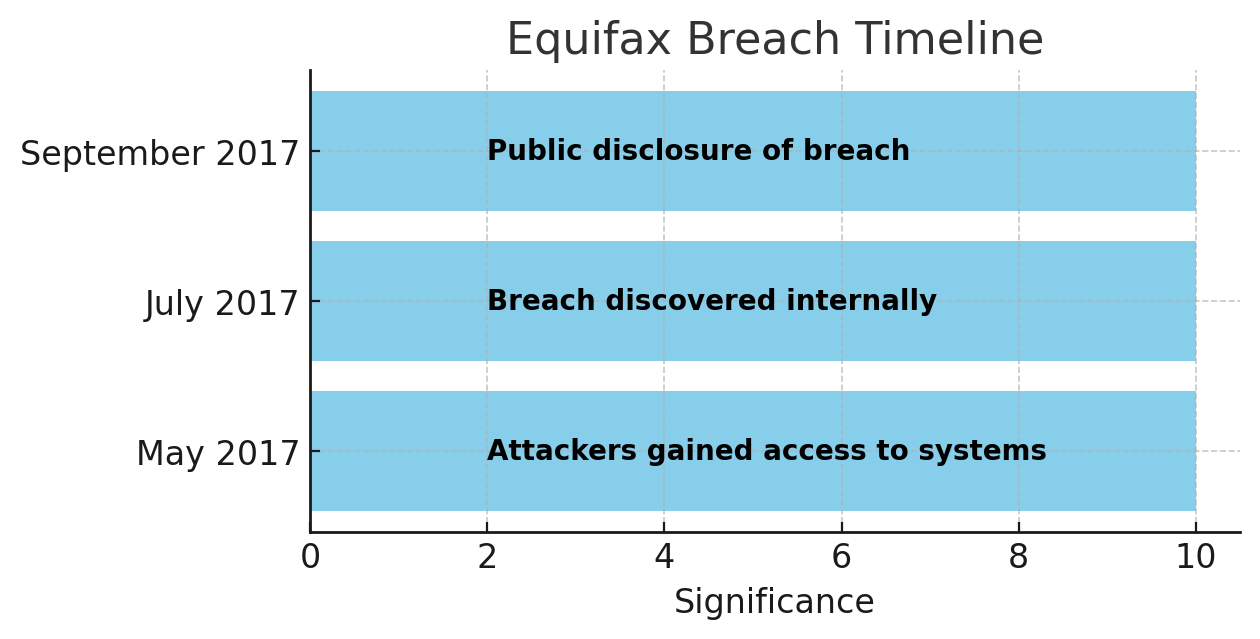
VULNERABILITIES

.

BREACH TIME LINE DIAGRAM

METHOD USED

* The following diagram illustrates the key events during the Equifax breach



T

* **Financial Impact:** Equifax incurred significant costs due to the breach, including fines, settlements, legal fees, and lost business. By the end of 2019, the company spent more than $1.4 billion in costs directly associated with the breach.
* **Personal Impact:** Over 147 million individuals had personal data exposed, including Social Security numbers, driver’s licenses, and credit card details.
* **Long-Term Consequences:** Victims faced increased risks of identity theft, fraud, and credit score manipulation.
* **Reputational Damage:** Trust in Equifax as a reliable credit agency plummeted, causing significant harm to its public image.
* **Legal Repercussions:** The breach led to numerous lawsuits and investigations, resulting in a $700 million settlement with the U.S. Federal Trade Commission (FTC).

ON STAKE HOLDER

ON CUSTOMER

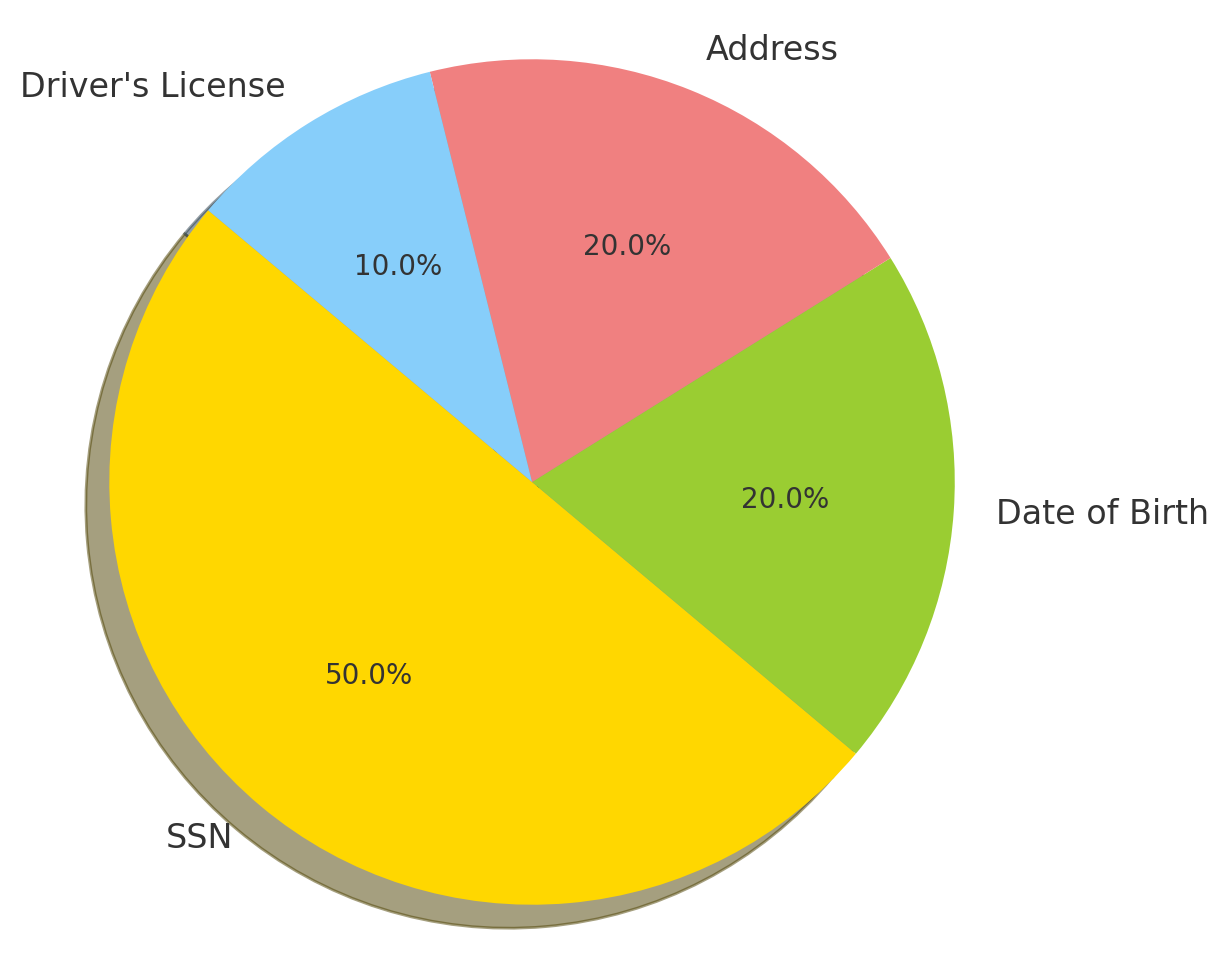
ON THE ORGANIZATION

IMPACT

TABLE IMPACT SUMMARY

|  |  |
| --- | --- |
| Affected Entity | Impact |
| Consumers | 147 million records exposed |
| Financial Impact | $1.4 billion in costs |
| Legal Impact | $700 million settlement with FTC |
| Reputational Damage | Trust erosion |

IMPACT OF BREACH DIAGRAM



MITIGATION

DISCOVERY

## **DISCOVERY ,MITIGATION STEP,CHANGES MADE**

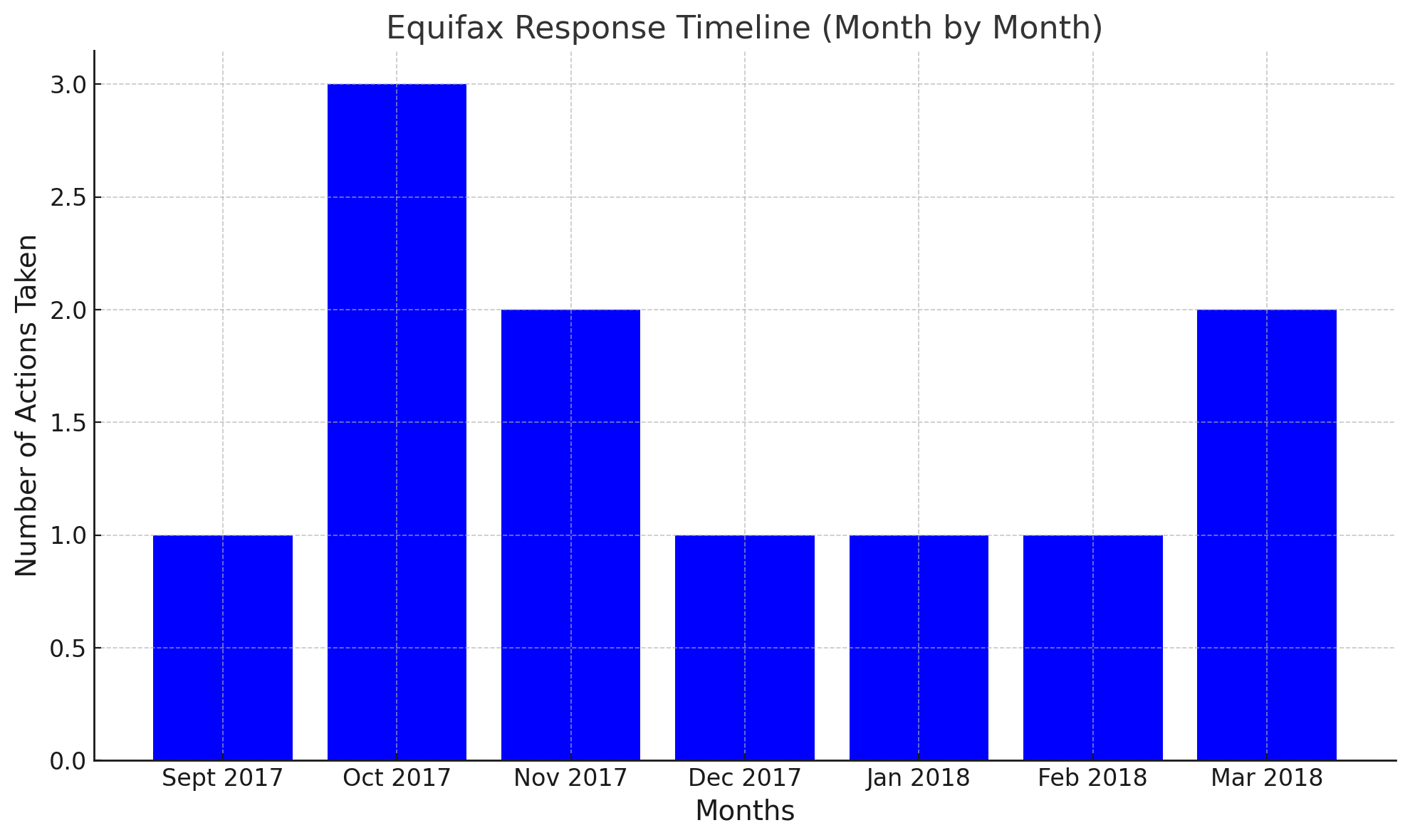
* The breach was discovered by Equifax on July 29, 2017, when security teams noticed unusual network activity.
* Equifax immediately took the affected application offline and hired a cybersecurity forensic team to assess the damage.
* They also offered free credit monitoring to affected consumers and implemented short-term security measures.

RESPONSE

Bar Graph: Equifax Response Timeline (Month by Month)

* **System Patches:** Applied critical patches to the exploited Apache Struts framework.
* **Improved Cybersecurity:** Equifax invested in a more robust security infrastructure, including enhanced encryption techniques and more sophisticated network monitoring tools.
* **Personnel Changes:** In the wake of the breach, Equifax’s CEO, CIO, and CISO resigned.
* **Regulatory Compliance:** Equifax committed to regular audits and implemented practices to comply with the GDPR and other regulatory frameworks.

CHANGES MADE



**Importance of Timely Patching:**

* Equifax’s failure to apply a patch led directly to the breach. Organizations must prioritize patch management to close security vulnerabilities promptly.

**Need for Segmented Systems:**

* Equifax’s lack of network segmentation allowed attackers to move freely within the system. Proper segmentation limits the scope of damage in case of an intrusion.

**Encryption of Sensitive Data:**

* Data encryption must be enforced to protect sensitive information. Even if a system is breached, encrypted data is far more difficult for attackers to exploit.

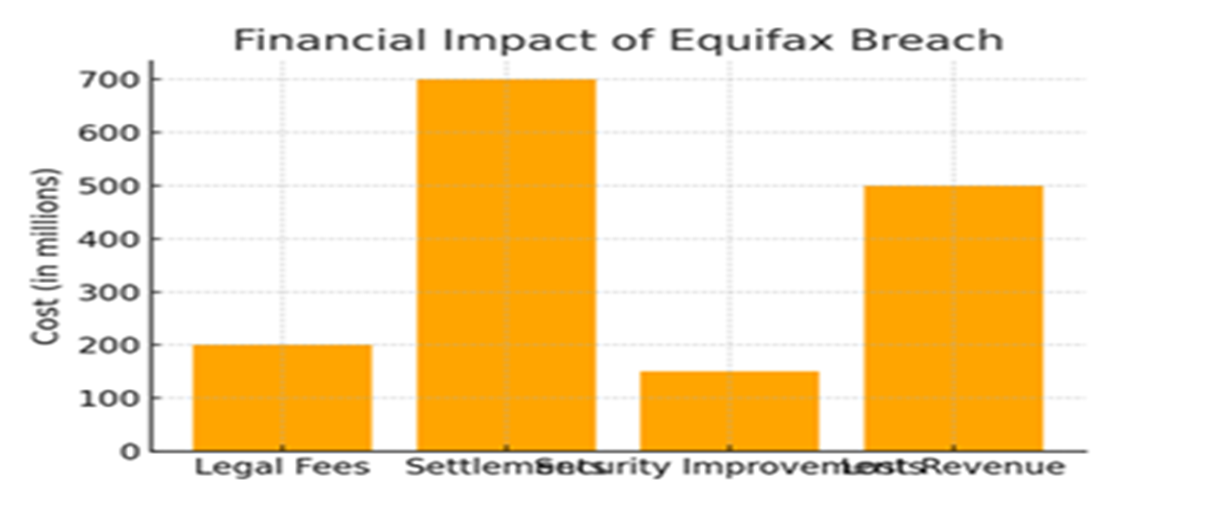
**Continuous Monitoring and Incident Response:**

* Equifax’s delayed detection of the breach highlights the importance of 24/7 monitoring and faster response times. Advanced threat detection tools should be deployed to detect anomalies immediately.

KEY TAKE AWAY & BEST PRACTICES

LESSONS LEARNED

BAR CHART OF FINANCIAL IMPACT OF EQUIFAX



* The Equifax data breach serves as a pivotal lesson in cybersecurity.
* It underscores the importance of timely software updates, network segmentation, and proactive monitoring in mitigating the risk of data breaches.
* While the company’s response addressed some immediate security vulnerabilities, the breach left lasting financial, reputational, and legal repercussions.
* The lessons learned from this incident offer valuable insights for improving data security strategies moving forward.

CONCLUSION

REFERENCES

* U.S. Federal Trade Commission (FTC), “Equifax Data Breach Settlement.”
* Verizon Data Breach Investigations Report (DBIR), 2018.
* "Equifax Data Breach: What Went Wrong?" Wired Magazine, 2017.