

|  |  |
| --- | --- |
| **Team members** | **Task Performed** |
| Jon Raihan |  |
| Aajith |  |
| Yong Hoow |  |
|  |  |

**Table of Contents**

**Section A (Findings)**

1. **The Incident**
2. **Context**
3. **Impact**
4. **How it Happened**

**Illustration of Equifax’s breach incident**

**Section B (Analysis)**

1. **Reflections**
2. **Future Improvements**

**Section C (Controls)**

1. **Preventive**
2. **Defective**
3. **Corrective**
4. **Justification**
5. **Conclusion**
6. **References**

# **SECTION A (FINDINGS)**

## **The incident**

A security and data breach at Equifax in 2017 exposed the financial and sensitive information of almost 147 million Americans.

For nearly 134 days, the hackers were able to remain unnoticed inside the Equifax computers.

## **Context**

The breach occurred between May and July 2017. It was caused by a vulnerability in Equifax's website that allowed hackers to access a web application that was used by consumers to dispute information on their credit reports. The hackers were able to access the application without a password, and they were able to download a large amount of data from the application.

Equifax did not discover the breach until July 2017, when it was notified by a security researcher. Equifax initially downplayed the severity of the breach, but it later acknowledged that it was one of the largest data breaches in history.

The Equifax data breach has had a significant impact on the lives of millions of people. Many people have had to take steps to protect their identities, such as placing a credit freeze on their credit reports. The breach has also led to calls for stricter regulations on data security.

The context of the Equifax data breach is important to understand because it shows how vulnerable our personal information can be. It also shows that companies need to be more proactive about security and that consumers need to be more aware of the risks of identity theft.

**Here are some of the key contextual factors that contributed to the Equifax data breach:**

* The vulnerability in Equifax's website was known for months before the breach. Equifax was aware of the vulnerability in its website in March 2017, but it did not take action to patch it. This was a major oversight, and it shows that companies need to be more proactive about security.
* Equifax's security practices were not up to par. Equifax's security practices were not up to par, and this contributed to the breach. For example, Equifax did not require employees to use strong passwords, and it did not have a strong incident response plan in place.
* The hackers were sophisticated. The hackers who exploited the vulnerability in Equifax's website were sophisticated. They were able to bypass Equifax's security controls and gain access to the company's data.
* By understanding the context of the Equifax data breach, we can learn from the mistakes that were made and take steps to prevent future breaches. We can also be more aware of the risks of identity theft and take steps to protect our personal information.

## **Impact**

Personal data of Equifax customers were comprised during these incidents. They are:

* Names
* Addresses
* Birth dates
* Social Security numbers (Similar to Singapore NRIC numbers)
* Driving licence number

In addition, about 209,000 credit card details and 182,000 sensitive documents were accessed by the intrusion.

As of 1st March 2018, it was reported that about 147 million personal details were accessed by this incident.[[1]](#footnote-2)

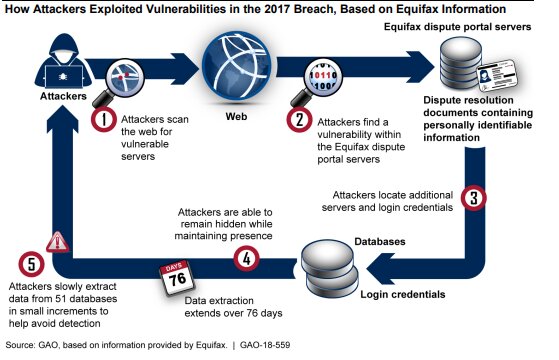
## **How it happened**

According to the United States Government Accountability Office inquiry[[2]](#footnote-3), it was initially hacked thru a consumer complaint web portal which the vulnerability (CVE-2017-5638) was not patched due to failure in Equifax internal processes.

The intruders were able to move from the web portal to other servers because the systems were not effectively segmented from one another, and usernames and passwords stored in plain text that then allowed them to access further systems.

The attackers pulled data out of the network in encrypted form undetected for months because Equifax had crucially failed to renew an encryption certificate on one of their internal security tools.

Equifax did not publicize the breach until more than a month after they discovered it had happened.



Section B (Analysis)

1. **Reflection.**

The Equifax data breach of 2017 was a major wake-up call for businesses and consumers alike. It showed how vulnerable our personal information can be, and how important it is to take steps to protect it.

Here are some of the key reflections from the Equifax data breach:

* Companies need to take data security seriously. Equifax was aware of the vulnerability in its website for months before the breach, but it did not take action to patch it. This was a major oversight, and it shows that companies need to be more proactive about security.
* Consumers need to be aware of the risks of identity theft. The Equifax data breach compromised the personal information of millions of people, including their Social Security numbers. This information could be used by criminals to commit identity theft, so it is important for consumers to be aware of the risks and take steps to protect themselves.

There is a need for stricter data security regulations. The Equifax data breach showed that the current patchwork of data security regulations is not enough. There is a need for stricter regulations that will hold companies accountable for their security practices.

The Equifax data breach was a major incident, but it can also be seen as an opportunity to learn and improve. By taking the lessons from this breach to heart, we can make our personal information more secure and help to prevent future breaches.

**Here are some additional reflections from the Equifax data breach:**

The breach highlighted the importance of having a strong incident response plan in place. Equifax was slow to respond to the breach, and this made it worse.

The breach also showed that companies need to be more transparent with their customers about data breaches. Equifax initially downplayed the severity of the breach, which eroded trust with its customers.

The breach has led to calls for a national data breach notification law in the United States. Currently, there is no federal law that requires companies to notify customers if their personal information has been compromised.

The Equifax data breach was a major event, but it is important to remember that it is not the only data breach that has happened. There have been many other large data breaches in recent years, and it is likely that there will be more in the future. The best way to protect yourself from data breaches is to be aware of the risks and take steps to protect your personal information.

1. **Future Improvement.**

Equifax has made several changes to its security practices in the wake of the 2017 data breach. These changes include:

* Investing in new security technologies. Equifax has invested in new security technologies, such as artificial intelligence and machine learning, to help detect and prevent future data breaches.
* Strengthening its security policies and procedures. Equifax has strengthened its security policies and procedures, including its incident response plan.
* Improving its employee training. Equifax has improved its employee training on data security.
* Communicating more transparently with customers. Equifax has committed to communicating more transparently with customers about data breaches.

These changes are a good start, but there is still more that Equifax can do to improve its security practices. For example, Equifax could:

* Be more proactive about patching vulnerabilities. Equifax should be more proactive about patching vulnerabilities in its systems.
* Do more to secure its data at rest and in transit. Equifax should do more to secure its data at rest and in transit.
* Work with other companies to share information about data breaches. Equifax should work with other companies to share information about data breaches so that they can learn from each other's experiences.

Section C (Controls)

To improve Equifax’s security practices, we are proposing 3 main areas of controls, preventive, defective and corrective.

1. **Preventive**

Preventive controls to avoid an incident from happening

### Administrative

1. Private web access
   1. Protect private information like Equifax systems using a susceptible version of Apache Struts web framework from being indexed by search engines. Put the information on private access website
2. Data retention policy
   1. Avoid storing sensitive information beyond the time necessary to provide the service. Unnecessary retaining of customer's information that was no longer needed lead to broader exposure of customer's information during an attack.
3. Update communication policy
   1. Equifax's IS team received alerts from the US Computer Emergency Readiness Team (US-CERT) about Apache Struts framework vulnerability on Mar 8, before the time of compromise on May 13.
   2. The person operating the Automated Consumer Interview System (ACIS) did not receive the alert as he/she was not part of the email recipient list. Thus, the patching process was not proactive.
   3. Recommendation: there should be a better communication policy between the IS and IT teams.
4. Executive priorities
   1. Executive compensation rules were focused on profit, motivating them to prioritize revenue above all other considerations, including information security. Thus, information security was not given much priority which could lead to security breaches.
   2. The recommendation is that IS and IT teams should report directly to either Chief Risk Officer, Chief Executive Officer or Chief Information Officer. This ensures security is represented at the executive level.
5. Security Awareness framework
   1. Request management to have company-wide cyber security management framework and ensure its adequate staffing and budget. Equifax can also share its latest security framework with other companies.

### Technical

1. Implement WAF and DLP system
   1. Equifax's Automated Consumer Interview System (ACIS) system comprises 2 web servers, 2 application servers and a network-level firewall. This system was open to accepting malicious requests as it was not protected by a WAF.
   2. A Web Application Firewall (WAF) is a layer of protection in addition to network-level firewall. It protects web applications from SQL injections, cross-site scripting (XSS) and distributed Denial of Service (DDoS) attacks. WAF could have prevented the exploitation of Apache Struts vulnerability.
   3. A Data Loss Prevention (DLS) system which identifies, monitors and potentially averts unauthorized moves of sensitive data in and out of the network. DLS could have prevented the massive exfiltration of 14-16 Gb of data for 76 days (about 2 and a half months) undetected.
2. Isolation or compartmentalization
   1. Computer sub-systems should be compartmentalized using physical devices or security controls. Equifax's Automated Consumer Interview System (ACIS) application was not segmented from other unrelated databases. The Sun systems, which hosted ACIS, had shared file systems, notes or configuration files from one system and can be accessed from other systems.
   2. Un-encrypted credentials to other sensitive databases were stored. Excessive amounts of confidential information and Personal Identifiable Information (PII) were also stored.
3. Encryption for Personal Identifiable Information (PII)
   1. None of the PII from the stolen data was encrypted, therefore compromising the confidentiality of the stolen PII. Encryption, truncation, masking or hashing of the critical PII is needed. Proper management of encryption keys can protect encrypted data. Even if encrypted data was stolen but encryption keys are not compromised, event is not considered a data breach.
4. Strong password
   1. Some Equifax's IT system privileged accounts have weak passwords. E.g., one database has a four lowercase-letter password which matched the name of the database. A portal used for credit dispute had username "admin" and password "admin" for an administrative account.
   2. The suggested strong password should be at least 12 characters long, a combination of uppercase, lowercase letters, numbers and symbols. Not a word that can be found in the dictionary, or name of a person, character, product or organization.
5. Least privilege access
   1. The principle of least privilege - every user in a system should be granted only a minimum set of permissions to perform the designated task.
   2. Equifax's Automated Consumer Interview System (ACIS) has excessive access to other systems not required for its operations. ACIS only needed access to 3 databases to function, but it was unnecessarily connected to many more.
6. Knowledge in use of vulnerability scanners
   1. The Equifax IS team scanned the system exposed to the internet using McAfee Vulnerability Manager tool. However, the scan was on the root directory, not the subdirectory where Apache Struts framework was listed.
   2. It was known that the detection rate of vulnerability scanners did not exceed 80% for most scans. Also, Apache Struts was not managed via a package manager but was distributed as a standalone JAR file.
   3. The identification of Apache Struts framework vulnerability also requires knowledge of the application URL path. When not provided, the scanner did not pick up the vulnerability.
   4. The IS team accepted the false-negative result as confirmation that Equifax's system did not have a problem.
7. Adopt Zero-trust security model
   1. The components of a system must mistrust all requests from other parts of the system until they are authenticated and authorized.
8. **Defective**

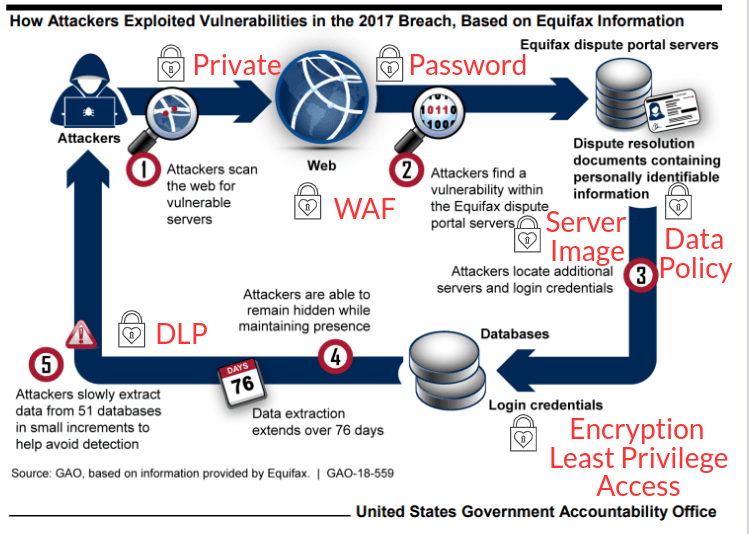
Defective controls detect an incident that has happened and help trace the perpetrators

### Technical

1. Logs
   1. Consult Mandiant (now part of Google cloud) security team. Both Equifax and Mandiant security teams analyzed digital forensic data. Investigators reconstructed every step: once the attackers found the vulnerability, they installed a backdoor known as a web shell.
   2. Eventually the intruders installed more than 30 web shells, each on a different web address. Groups known to exploit with web shells most effectively include teams with links to Chinese Intelligence. In total, the attackers ran approximately 9,000 queries on Equifax’s system, obtaining names, birth dates and social security numbers for nearly 145 million Americans. Wu Zhiyong, Wang Qian, Xu Ke and Liu Lei, members of the PLA’s 54th Research Institute, a component of the Chinese military were charged.
2. Intruder Detection and Prevention System (IDS/IPS)
   1. Automated SSL certification management tool was implemented but not completed before the hacking incident. Avoid manual process of tracking and updating several hundred SSL certificates. This process was error prone and depended on the individual responsible for IT systems.
   2. Equifax's IDS/IPS was not able to detect malicious traffic leaving the system due to an expired SSL certificate in Nov 2016.
   3. Lack of alerts to the IS team that the IDS/IPS was not operational for 9 months (until July 2017). Lack of warning possible as system settings allow traffic to bypass IDS/IPS in case it was unable to function.
3. **Corrective**

Corrective controls fix components or systems after an incident has happened.

1. Server Images
   1. One way to correct online servers infected by malware is restoring from offline server images, which remain untouched by the threat actors.
2. Real time recovery
   1. Cloud based backup of server data where user can restore data to the time point before the malware was inserted.



**Preventive Control Costs**

|  |  |  |
| --- | --- | --- |
| **Control** | **Role / Product** | **Cost per year ($)** |
| Private web access | new web developer | 65,000 |
| Data retention policy | new data analyst | 70,000 |
| Update communication policy | IT staff | --- |
| Executive priorities | Executive committee | --- |
| Security awareness framework | CIO, IT, IS teams | --- |
| Web Application Firewall (WAF) | Microsoft | 1,080 |
| Data Loss Protection (DLP) | ManageEngine | 795 |
| System compartmentalization | new system engineer | 100,000 |
| Encryption and strong password | new IT administrator | 80,000 |
| Least privilege access | new database administrator | 60,000 |
| Vulnerability scanner | refresher training | --- |
| zero-trust security model | CIO, IT, IS teams | --- |

**Defective Control Costs**

|  |  |  |
| --- | --- | --- |
| **Control** | **Role / Product** | **Costs per year ($)** |
| Network logs forensics | Mandiant (now part of Google cloud) | 50,000 |
| SSL management tool | Solar Winds | 3,346 |

**Corrective Control Costs**

|  |  |  |
| --- | --- | --- |
| **Control** | **Role / Product** | **Costs per year ($)** |
| Server Images | Acronis | 999 |
| Real time recovery system | Arcserve | 1,000 |

1. **Justification**

We recommend using more money and human resources in implementing preventive controls to improve the security of Equifax. In this way, it can prevent most of the data breaches from occurring at the first place. Our stand is that prevention protects the loss of trust in the company, the risks to customers whose data was stolen and the heavy fines the company is liable for.

However, on the event that a data breach occurs, there will still be defective and corrective controls in place to recover from the attack.

1. **Conclusion**

The loss or unauthorised leak of information in a data breach can lead to serious consequences and can result in substantial harm to customers and reputation loss to the company.

As prevention is better than cure, businesses should not neglect the cyber security part of the business.

1. **References**

<https://controlsframework.equifax.com/home>

<https://www.equifax.com/newsroom/all-news/-/story/how-equifax-shaped-the-future-of-cybersecurity-in-2022/>

<https://assets.equifax.com/marketing/US/assets/2022-security-annual-report.pdf>

<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3957272>

<https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf>

1. [↑](#footnote-ref-2)
2. [↑](#footnote-ref-3)