# ELEC-E7470 –Cybersecurity

## (Group Work – Case Study Article)


**Jaspreet Walia** **467355**

**Venkatesh Kulkarni** **722281**

**Soumadipta Pyne** **725631**

**14/05/2019**

# Contents

# Abstract

Equifax, founded 1899, is one of three biggest credit rating agencies, with thousands of employees and operations in many countries around the world. Equifax helps other companies and individuals make informed decisions by providing credit monitoring and fraud-prevention services. Like any other company in this industry, Equifax holds a vast amount of privacy sensitive data on consumers. The vast reach of the company's operations, services and client base make them a big target for cyber criminals looking for valuable data. The company has had its share of data related controversies since the 1960s and more recently a massive breach in 2017 involving 150 million people that brought shade to company's data handling once again. Through this article we follow the Equifax data breach of 2017, starting from the company's early years, past controversies, the causes and impacts of the breach and the company's response. Then, we provide our analysis of the breach and what could have been done. The events that lead to this breach, the massive scale and impact of the breach, and the malpractices on the company's end make this a very interesting and engaging case study from cybersecurity perspective.


# 1 Introduction

The term "cybersecurity" is broadly used in today's world and the range of definition of this term varies hugely and is often subjective. The term has been an area of interest not only in the world of academics but also in industry, government and non-government organizations. Cybersecurity is made of two words, Cyber and security. Also, commonly used or in some cases misused terms for the same field are computer security, IT security, and information security. To understand the big picture about cybersecurity, it is important to know the components of related security aspects [1]. The term cybersecurity is mainly composed of two different words: 'Cyber' relates to the use of computers and information and communication technology. 'Security' relates to the security against the risks of using various 'cyber' components. Thus, the various components of cybersecurity include, typically, Network security, Application security, Endpoint security, Data security, Identity management, Database and infrastructure security, Cloud security, Mobile security, Disaster recovery/business continuity planning, and End-user education.

Recent hacks and data breaches have pulled more attention to cybersecurity and the term that was a concept a few decades ago is a well used and crucial aspect of today's connected life. For our case study we have chosen a massive data breach incident that has been labelled as the largest corporate data breach in US history – 'The Equifax data breach 2017'. The whole paper has been divided into 8 sections. First, we have given the background of the company, then we discussed about the breach and what was stolen, next we talk about who was responsible and where is all the data and what caused the breach. In the later section we have discussed about the company's response to the breach, impacts of the breach. Finally we tried to find out what the company could have done to minimize the damage.

# 2 About Company

Equifax Inc. is a data analytics and technology company that helps individuals and organizations make informed business and personal decisions. Equifax serve as a consumer advocate, financial literacy steward, and economic advancement champion. As an innovative global information solutions company that allows access to credit, Equifax is a part of breakthrough collaborations and innovations that address complex social challenges for underprivileged youth such as social welfare, community relationships and financial education [2].

The company was founded by Cator and a guy named Woolford in Atlanta, Georgia, United States in the year 1899. It is one of the three largest credit agencies along with Experion and TransUnion. The company flourished very quickly and had offices throughout the United States and Canada by the year 1920. While the company continued to report on credit, most of their business was reporting to insurance companies when people applied for new insurance policies including life, auto, fire, and medical insurance [3]. All major insurance companies used RCC to obtain health, habits, morals, vehicle and finance information. They also investigated claims for insurance and made job reports when people were looking for new jobs. A subsidiary, Retailers Commercial Agency, then performed most of the credit work.

Equifax had an extensive information holding and what was unethical on their part was their willingness to sell the information to anyone. This started to hamper the company in a negative way in the year 1960s and 1970s. These included collecting "... facts, statistics, inaccuracies and

rumors ... about virtually every phase of a person's life; his marital disorders, jobs, school history, childhood and political activities." As a result, in 1970, Congress held hearings. This led to the enactment of the same year's Fair Credit Reporting Act that gave consumers rights to information stored about them in corporate data banks. The hearings are alleged to have prompted the Retail Credit Company in 1975 to change their name to Equifax to improve their image [3].

# 3 The breach in 2017

A massive data breach was discovered in the month of July 2017 at Equifax which compromised the personal information of around 150 Million people as reported [4]. The company says the breach started in mid-May. When Equifax notified about the breach in September 2017, it immediately hit the headlines and has become a topic of discussion since then [5]. The breach is considered to be the largest corporate data breach in US history where not only clients of US but clients from Canada and Australia were also affected.

Although no data breach should be taken lightly, Equifax being a consumer credit reporting agency made it worse because it involved sensitive personal identifiable information. According to a report the stolen data included social security number, name, address, date-of-birth, driver's license information and around 209,000 credit card numbers. Figure 1 shows a detailed statistic of what was stolen [6].

Data held by Equifax was accessed by hackers through a web application vulnerability for which a well-known patch was available. The Equifax website is built on software called 'Apache Struts', a widely used framework for creating programs that helps company manage a large amount of data online. In March, the Apache foundation which oversees struts announced the existence of a vulnerability in the software code that they dubbed CVE-2017-5638. Almost everyone nowadays has filled up the web form numerous time to order product, register for accounts etc. But because of a bug in the way struts handled data entered to those forms, hackers could use them to send the malicious code to the service with the data on them. This type of hack is called the remote code execution.

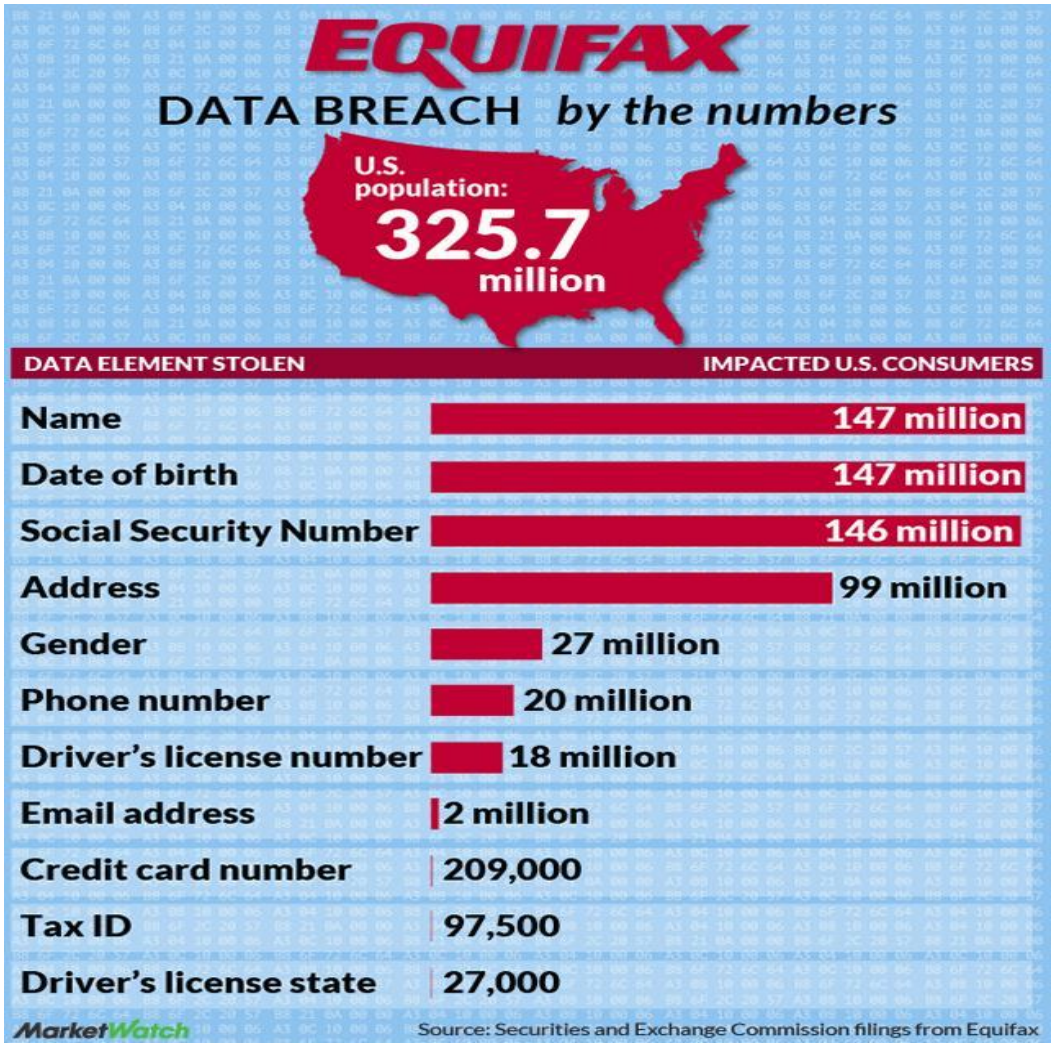


**Figure 1 Equifax Data Breach 2017**

Normally, programmers protect against this type of hack by having the server check what you are doing and submitting to make sure its not computer code. But with this vulnerability, hackers could trigger an error, then make the server run the embedded commands while it was trying to figure out what the error was.

# 4 Who is responsible for the breach and what did they do with the data?

Chinese spies are expected to behind this breach. They were likely to use this data to exploit traditional path of identity theft by opening fraudulent accounts using victims personal information. The attackers might have used data to transfer funds or physically move money from one account to another [7]–[9].

# 5 What caused the breach?

When the company announced in July 2017 that criminals had expoited a US web application vulnerability to access their files. The main casue as identified by many reports and by the company's CEO was the delay or inability to implement a fix in a web application tool called Apache Struts. The company's culture can be a reason for the negligence to apply a fix they had been aware of.

According United State Government Accountability Office (GAO) investigation the attackers followed the procedure shown in Figure 2.

Apache Struts is a open source web application framework, first released in 2000, is used by web developers for Java EE web applications adopting a model/view controller architecture [11]. The Apache foundation had a sin off called WebWork framework that developed further to enhance the exisiting framework while keeping the original architecture. Later, in 2007 the WebWork framework got adopted as Apache Struts 2. Apache struts 2 is the framework version that was used by the Equifax web developers.

Typical Java EE web applications work by providing the client with access to the database via a web form but this is inadequate as it mixes the application logic with presentation and thus makes maintenance difficult. Apache Struts firslty tries to solve this problem by separating the application logic, the prresented HTML pages to the client and the instances for passing the information between the logic and the client. Then it facilitates templayte writing for the presentation and binding together the web developers code with the presentation. So when the client requests are sent, it responds by interacting with the appropriate application logic to return the requested page.

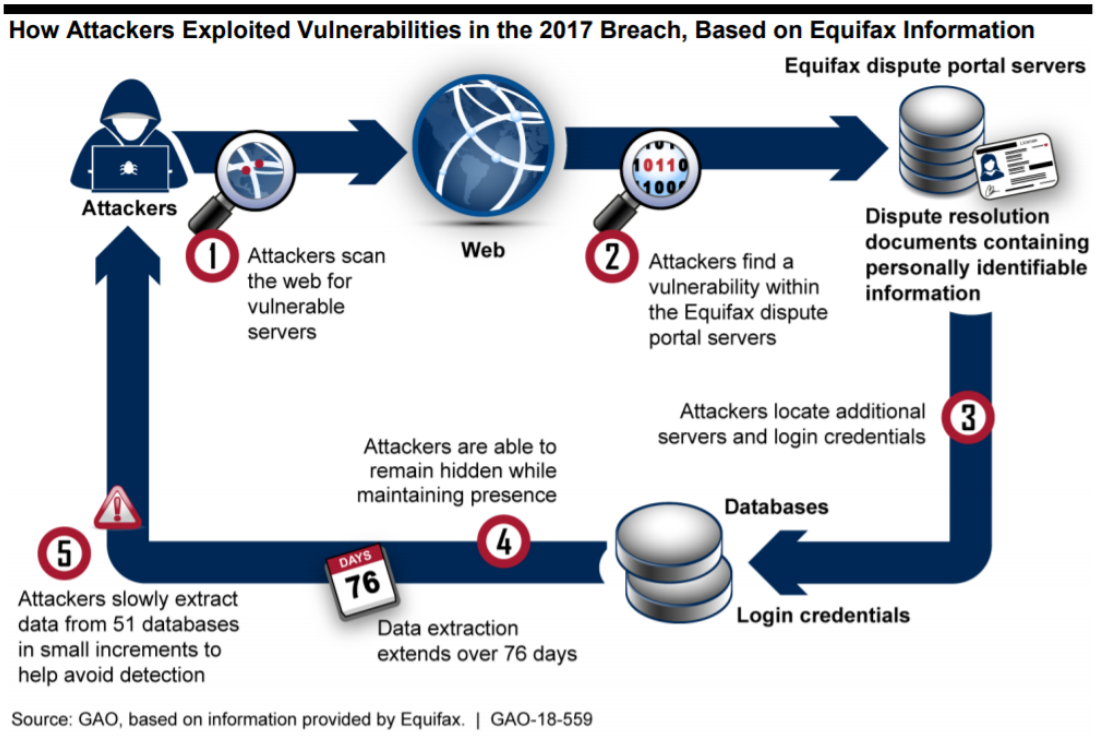


**Figure 2 The Equifax data breach 2017 [10]**

Addionally this version uses Object-Graph Navigation Language (OGNL) technology. OGNL allows for simplere array manipulation, use simpler expressions to get and set properties and execution of methods. OGNL also allows programs to change behavior based on object graph state instead of relying on compile time settings. Due to its ability to change executable code OGNL adds a critical security flaw, particularly to execute arbitrary code. Due to this flaw users are urged to regularly update to avoid documented vulnerabilities [12].

Apache Struts 2, the Struts version in question has had many critical vulnerabilities in the past. Past versions such as 2.3.5 to 2.3.31, 2.5 to 2.5.10 allow remote attackers to execute arbitrary code [13]. According to CVE Details vulnerability database [14], Apache Struts 2 has had 70 vulnerabilities with none of them requiring any form of authentication. The datbase also score the vulnerabilities out of 10, with 10 being the most critical. Out of these 70 about 14 vulnerabilities have been scored above 9, and 3 vulnerabilities scored a full 10.

| # | CVE ID | CWE ID | # of Exploits | Vulnerability Type(s) | Publish Date | Update Date | Score | Gained Access Level | Access | Complexity | Authentication | Conf. | Integ. | Avail. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | CVE-2018-11776 | 20 | | Exec Code | 2018-08-22 | 2019-01-16 | 9.3 | None | Remote | Medium | Not required | Complete | Complete | Complete |
| | Apache Struts versions 2.3 to 2.3.34 and 2.5 to 2.5.16 suffer from possible Remote Code Execution when alwaysSelectFullNamespace is true (either by user or a plugin like Convention Plugin) and then: results are used with no namespace and in same time, its upper package have no or wildcard namespace and similar to results, same possibility when using url tag which doesn't have value and action set and in same time, its upper package have no or wildcard namespace. | | | | | | | | | | | | | |
| 2 | CVE-2018-1327 | 20 | | | 2018-03-27 | 2018-07-18 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| | The Apache Struts REST Plugin is using XStream library which is vulnerable and allow perform a DoS attack when using a malicious request with specially crafted XML payload. Upgrade to the Apache Struts version 2.5.16 and switch to an optional Jackson XML handler as described here http://struts.apache.org/plugins/rest/#custom-contenttypehandlers. Another option is to implement a custom XML handler based on the Jackson XML handler from the Apache Struts 2.5.16. | | | | | | | | | | | | | |
| 3 | CVE-2017-12611 | 20 | | | 2017-09-20 | 2017-09-29 | 7.5 | None | Remote | Low | Not required | Partial | Partial | Partial |
| | In Apache Struts 2.0.1 through 2.3.33 and 2.5 through 2.5.10, using an unintentional expression in a Freemarker tag instead of string literals can lead to a RCE attack. | | | | | | | | | | | | | |
| 4 | CVE-2017-9805 | 502 | | Exec Code | 2017-09-15 | 2017-11-09 | 6.8 | None | Remote | Medium | Not required | Partial | Partial | Partial |
| | The REST Plugin in Apache Struts 2.1.2 through 2.3.x before 2.3.34 and 2.5.x before 2.5.13 uses an XStreamHandler with an instance of XStream for deserialization without any type filtering, which can lead to Remote Code Execution when deserializing XML payloads. | | | | | | | | | | | | | |
| 5 | CVE-2017-9804 | 399 | | | 2017-09-20 | 2018-06-30 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| | In Apache Struts 2.3.7 through 2.3.33 and 2.5 through 2.5.12, if an application allows entering a URL in a form field and built-in URLValidator is used, it is possible to prepare a special URL which will be used to overload server process when performing validation of the URL. NOTE: this vulnerability exists because of an incomplete fix for S2-047 / CVE-2017-7672. | | | | | | | | | | | | | |
| 6 | CVE-2017-9793 | 20 | | | 2017-09-20 | 2018-06-30 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| | The REST Plugin in Apache Struts 2.3.7 through 2.3.33 and 2.5 through 2.5.12 is using an outdated XStream library which is vulnerable and allow perform a DoS attack using malicious request with specially crafted XML payload. | | | | | | | | | | | | | |
| 7 | CVE-2017-9791 | 20 | | Exec Code | 2017-07-10 | 2018-07-07 | 7.5 | None | Remote | Low | Not required | Partial | Partial | Partial |
| | The Struts 1 plugin in Apache Struts 2.3.x might allow remote code execution via a malicious field value passed in a raw message to the ActionMessage. | | | | | | | | | | | | | |
| 8 | CVE-2017-9787 | 284 | | | 2017-07-13 | 2018-07-07 | 5.0 | None | Remote | Low | Not required | None | None | Partial |
| | When using a Spring AOP functionality to secure Struts actions it is possible to perform a DoS attack. Solution is to upgrade to Apache Struts version 2.5.12 or 2.3.33. | | | | | | | | | | | | | |
| 9 | CVE-2017-7672 | 20 | | | 2017-07-13 | 2018-07-07 | 4.3 | None | Remote | Medium | Not required | None | None | Partial |
| | If an application allows enter an URL in a form field and built-in URLValidator is used, it is possible to prepare a special URL which will be used to overload server process when performing validation of the URL. Solution is to upgrade to Apache Struts version 2.5.12. | | | | | | | | | | | | | |
| 10 | CVE-2017-5638 | 20 | | Exec Code | 2017-03-10 | 2018-03-03 | 10.0 | None | Remote | Low | Not required | Complete | Complete | Complete |
| | The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception handling and error-message generation during file-upload attempts, which allows remote attackers to execute arbitrary commands via a crafted Content-Type, Content-Disposition, or Content-Length HTTP header, as exploited in the wild in March 2017 with a Content-Type header containing a #cmd= string. | | | | | | | | | | | | | |
| 11 | CVE-2016-8738 | 20 | | | 2017-09-20 | 2018-06-30 | 4.3 | None | Remote | Medium | Not required | None | None | Partial |
| | In Apache Struts 2.5 through 2.5.5, if an application allows entering a URL in a form field and the built-in URLValidator is used, it is possible to prepare a special URL which will be used to overload server process when performing validation of the URL. | | | | | | | | | | | | | |
| 12 | CVE-2016-6795 | 22 | | Exec Code Dir. Trav. | 2017-09-20 | 2018-06-30 | 7.5 | None | Remote | Low | Not required | Partial | Partial | Partial |

**Figure 3 CVE Details, List of Vulnerabilities in Apache Struts 2 (Screenshot) [14]**

The CVE-2017-5638 vulnerability in Apache Struts 2 was advised to Equifax in March 2017 but Equifax failed to update to the newer version. This vulnerability as highlighted in the screenshot from CVE details website (Figure 3) [14], affected 53 of Apache Struts 2 product versions [15] being used at that time and users were advised to update to the latest secure version at that time. This vulnerability that allows attackers to execute arbitrary code has the impacts as listed in Table 1.

In September 2017, Equifax reported the data breach, and in a later report it was blamed on the Apache struts 2 vulnerability from March 2017. This vulnerability let even any attackers with low skills to completely compromise the confidentiality, integrity and availability of information in Equifax's database. Moreover, there was no authentication required to take advantage of this vulnerability. Equifax was advised to apply the fixes but it failed to do so, which can be blamed on their negligence, lack of responsibility and resources. This highly reflects on the culture of the company and their historically long tradition to take user privacy and cybersecurity lightly [3].

**Table 1 List of Impacts of the Apache Struts 2 Vulnerability from March 2017 [15]**

| Type of Impact | Description |
|---|---|
| Confidentiality Impact | Complete<br>(There is total information disclosure, resulting in all system files being revealed.) |
| Integrity Impact | Complete<br>(There is a total compromise of system integrity. There is a complete loss of system protection, resulting in the entire system being compromised.) |
| Availability Impact | Complete<br>(There is a total shutdown of the affected resource. The attacker can render the resource completely unavailable.) |
| Access Complexity | Low<br>(Specialized access conditions or extenuating circumstances do not exist. Very little knowledge or skill is required to exploit.) |
| Authentication | Not required<br>(Authentication is not required to exploit the vulnerability.) |

Multiple other reports have pointed out more factors that lead to the data breach:

- Insecure network design without proper segementation [16]
- Inadequate encryption of Personally Identifiable Information (PII) [17]
- Ineffective breach detection mechanisms [18]

Network segmentation is a crucial part of network design to isolate multiple department networks not just for independent management but also control access between departments and between personnel and non-personnel. To safeguard private data it is important to encrypt the data even if it is stored on private servers because otherwise in case of a data breach the data can be easily read

and manipulated. Absence of effective breach detection mechanisms can lead to data breaches going unnoticed for a long time.

According to the report by GAO [10], the attackers gained access to an online dispute portal through which they were able to send queries and commands to retrieve PII from their systems. This way they were able disguised their presence on the Equifax network, without being detected by Equifax's detection mechanism. The attackers were further able to gain access to more unencrypted PII, using these usernames and password the attackers were able to gain further access to more databases. The attackers ran about 9000 queries and were able to access 51 databases. This attack lasted 76 days before it was finally discovered.

This attack represents a type of event that could have been avoided with proper cybersecurity measures and following basic practices. The inability to apply a fix even after being notified about the vulnerability and poor network and data management reflects highly on their poor expertise and negligence on basic practices.

# 6 Company's response

Equifax took two months to notify the public about the breach. After the breach was made official to public the chief executive officer issued an apology stating, "***This is clearly a disappointing event for our company and one that strikes at the heart of who we are and what we do. I apologize to consumers and our business customers for the concern and frustration this causes," said Chairman and Chief Executive Officer, Richard F. Smith. "We pride ourselves on being a leader in managing and protecting data, and we are conducting a thorough review of our overall security operations. We also are focused on consumer protection and have developed a comprehensive portfolio of services to support all U.S. consumers, regardless of whether they were impacted by this incident***" [19].

There was a lack of clarity as to what data was impacted and the intent of the attackers behind the breach. The lack of transparency resulted in heavy criticism from media and public. Customers were left in a panic state, as they were not sure if they were affected and to what extent. Equifax

allows people to check if they are impacted by setting up a website that asked for customer's last name and last six digits of social security number [6].

However, there have been issues with the website itself with many users claiming of not getting a clear response and other questioning its validity. It was found that even fake last name and social security number led to the message saying that their data might have been compromised. The website was found to be vulnerable and it was easily possible for a hacker to trick a user into phishing, tricking user into loading site from a malicious link. Equifax included an arbitration clause in which people who use the website to check if there data has been compromised waive their rights to file class-action suits against them [21]. They also engaged a leading cybersecurity firm to conduct a comprehensive forensic review/analysis to unearth the scope of attack and to know the specific data that is impacted. Customer service support was extended over the weekends for the customers to help clarify their queries and actions that could be taken. Company later sent emails to customers directly whose data was compromised in the attack.

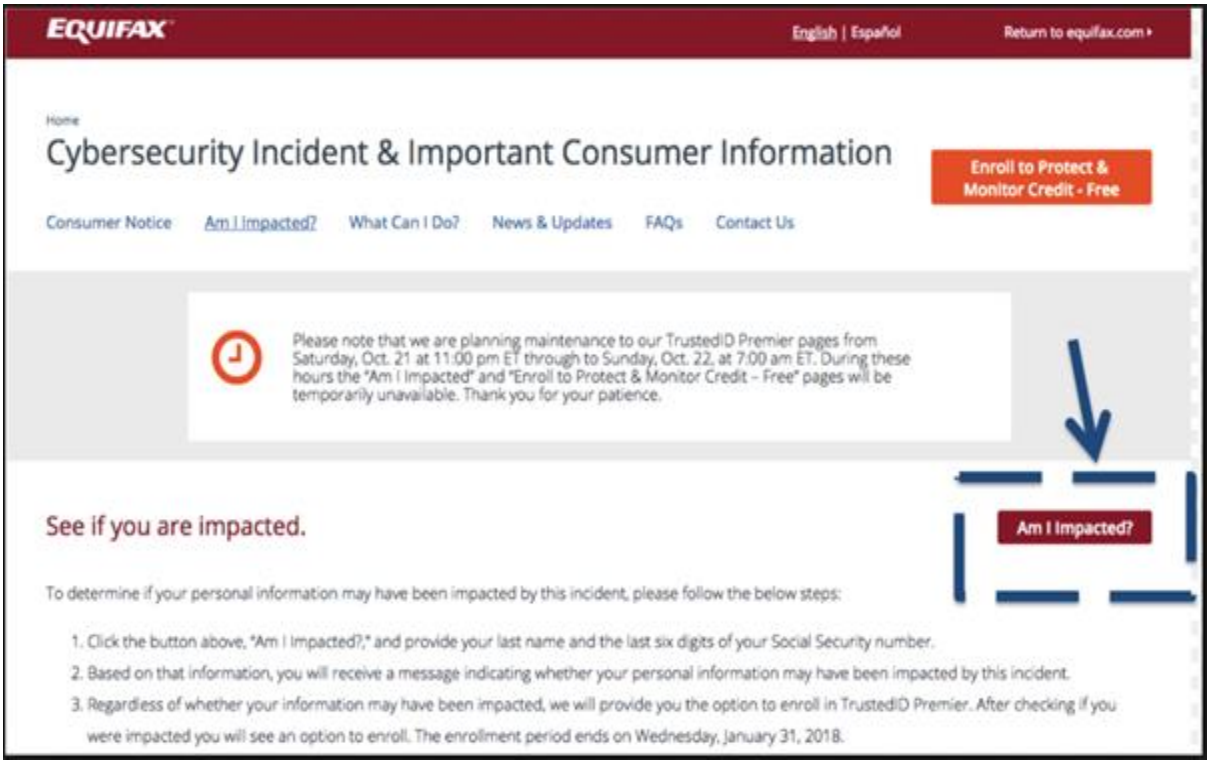


**Figure 4 Screenshot of the website set up by Equifax [20]**

Equifax handled the whole attack poorly. High-level executives including company's chief financial officer sold off almost two million shares just days after they came to know about the attack before even making it public. It affected the company heavily and their stock prices plummeted [21].

Equifax discovered that a misconfiguration allowed encrypted traffic to pass through the network without being inspected which was due to an expired digital certificate. Post the attack, Equifax corrected the misconfiguration blocking several internet addresses. During the inspection, they got to know the signs of intrusion. Commands were executed from several internet addresses that were not part of normal operations [10].

To further assess the scope of the data breach Equifax used electronic logs that had not been erased by the attackers to record the commands that they executed to retrieve the confidential data. It also helped them to know what kind of data has been compromised and the company also notified Federal Bureau of investigation about the breach [10].

To prevent such attacks in the future Equifax officials stated that new system-level measures were implemented to address the vulnerabilities that lead to the breach. It is also making changes in their management process to identify, patch and verify software vulnerabilities. Equifax officials also stated that they have developed new policies protect their data and implemented tools to continuously monitor the traffic data. They also took measures to monitor communications outside the company's boundary and added restrictions on traffic between internal servers. They implemented new security control framework for accessing specific applications and networks. Lastly, Equifax implemented a new endpoint security system to detect misconfigurations, to automatically notify potential threats/vulnerabilities to the system administrators.

# 7 The impacts of the breach

Equifax handled the breach poorly consequently it had negative impacts on the company. It faced approximately 240 individual class-action lawsuits and more than 60 investigations involving US, UK and Canada government agencies. The website set up for customers to check if their data has been compromised did not help either creating confusion among users. Equifax lost senior executive officers and the share price dropped by 18 % after the breach was made public eventually losing customer trust [22]. Equifax also stated that breach costed them around 300 million in non-recurring costs. Most of this money was invested in improving company's security and information technology.

The Figure 5 shows the impact of the breach on share price. It could be seen that share price has recovered much of its losses since the attack.

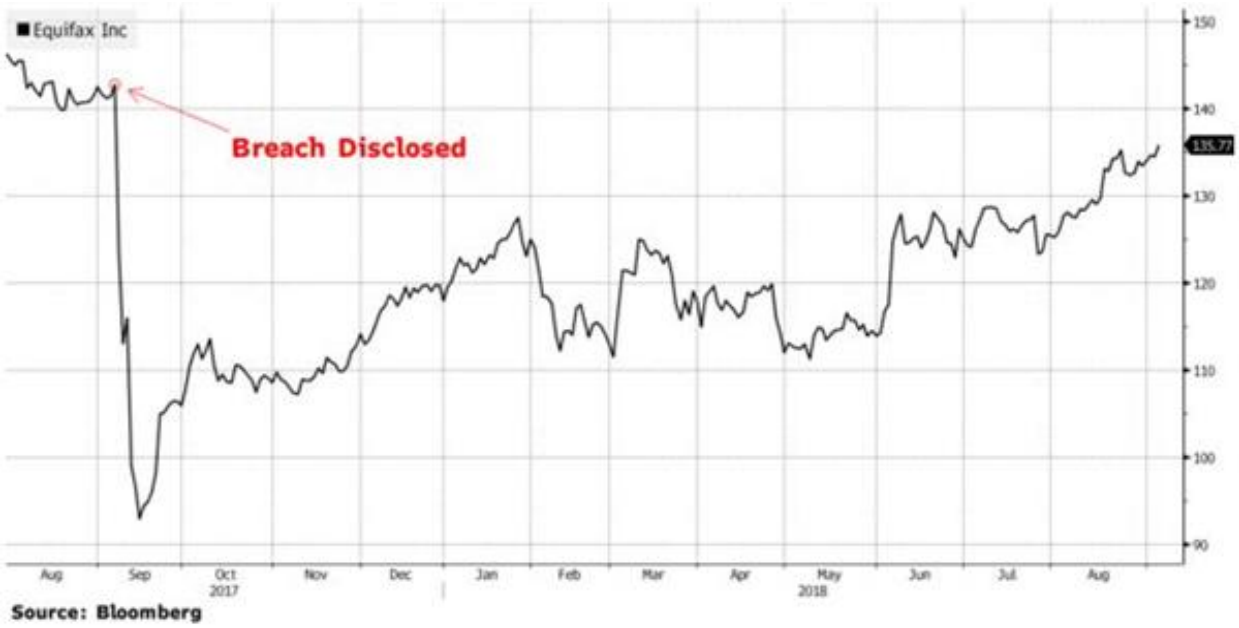


**Figure 5 Impact of data breach on company share price**

Equifax has a tough task to convince people that there will not be breach of same magnitude again majorly because of the way they reacted to the breach.

# 8 What could have been done?

The breach could have been avoided because Equifax were aware of the fix which had to be implemented in the Apache struts tool that they use even before the breach happened but they failed to do it in time. This breach was not due to a technical issue as the fix was already available. Equifax officials stated that an expired digital certificate about 10 months before breach occurred allowed attackers to execute commands and steal the confidential data without detection.Equifax had the required resources to install the fix in time but they clearly did not have the right culture, policies, management to be followed in installing it and address the known vulnerability. Lack of proper security culture and negligence resulted into a breach. The way Equifax responded to the breach could have been improved. For instance Equifax on its official twitter account tweeted a phishing link four times instead of the actual response page but luckily the page was not actually malicious. They failed to follow process which made them commit mistakes repeatedly [23].

# 9 Conclusions

The Equifax breach was unique in its own way and offers major learning for all the business organisations. It is an eye opener for organisations to increase cybersecurity measures in preventing such attacks. One major take away from this breach is about responding to such high magnitude attacks and also showing your customers about the measures that are undertaken to improve security through open communication, customer support and commitment to transparency [24]. There have been many such cyber attacks in the recent past and companies are left confusing about how to protect their organisation. Cyber attacks need a thorough investigation to determine the impact and to take necessary actions to resolve it with utmost priority. Developing proactive disaster recovery plans by regularly verifying the systems for vulnerabilities , active monitoring can help organisations to tackle such attacks and lower the risk of data breaches in future.

# References


[1] “What is Cyber Security? Definition, Best Practices & More | Digital Guardian.” [Online]. Available: https://digitalguardian.com/blog/what-cyber-security. [Accessed: 27-Apr-2019].

[2] “About Us | Equifax.” [Online]. Available: https://www.equifax.com/about-equifax/. [Accessed: 14-May-2019].

[3] “Separating Equifax from Fiction | WIRED.”

[4] “Equifax says website vulnerability exposed 143 million US consumers | CSO Online.” [Online]. Available: https://www.csoonline.com/article/3223229/equifax-says-website-vulnerability-exposed-143-million-us-consumers.html. [Accessed: 19-Apr-2019].

[5] “Case Study: The Equifax Breach | IT Security Training Australia.” [Online]. Available: https://www.itsecuritytraining.com.au/articles/case-study-equifax-breach. [Accessed: 14-May-2019].

[6] “Case Study: Equifax Data Breach | Packetlabs.” [Online]. Available: https://www.packetlabs.net/equifax_data_breach/. [Accessed: 12-May-2019].

[7] “Council Post: The Equifax Data: Now That They Have It, How Will Hackers Use It?” [Online]. Available: https://www.forbes.com/sites/forbestechcouncil/2017/11/29/the-equifax-data-now-that-they-have-it-how-will-hackers-use-it/#430b214602cd. [Accessed: 12-May-2019].

[8] “Before Breach, Equifax Suspected Chinese Spies | PYMNTS.com.” [Online]. Available: https://www.pymnts.com/news/security-and-risk/2018/data-breach-equifax-china-spying/. [Accessed: 12-May-2019].

[9] “It’s China behind Equifax Cyber Attack! - Cybersecurity Insiders.” [Online]. Available: https://www.cybersecurity-insiders.com/its-china-behind-equifax-cyber-attack/. [Accessed: 12-May-2019].

[10] “DATA PROTECTION Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach Report to Congressional Requesters United States Government Accountability Office,” 2018.

[11] “Welcome to the Apache Struts project.” [Online]. Available: https://struts.apache.org/. [Accessed: 11-May-2019].

[12] “OGNL - Wayback Machine.” [Online]. Available: https://web.archive.org/web/20081025020323/http://www.ognl.org/. [Accessed: 11-May-2019].

[13] “Critical vulnerability under ‘massive’ attack imperils high-impact sites [Updated] | Ars Technica.” [Online]. Available: https://arstechnica.com/information-technology/2017/03/critical-vulnerability-under-massive-attack-imperils-high-impact-sites/. [Accessed: 11-May-2019].

[14] “Apache Struts : List of security vulnerabilities.” [Online]. Available: https://www.cvedetails.com/vulnerability-list.php?vendor_id=45&product_id=6117&version_id=&page=2&hasexp=0&opdos=0&opec=0&opov=0&opcsrf=0&opgpriv=0&opsqli=0&opxss=0&opdirt=0&opmemc=0&ophttprs=0&opbyp=0&opfileinc=0&opginf=0&cvssscoremin=0&cvssscoremax=0&ye. [Accessed: 11-May-2019].

[15] “CVE-2017-5638 : The Jakarta Multipart parser in Apache Struts 2 2.3.x before 2.3.32 and 2.5.x before 2.5.10.1 has incorrect exception ha.” [Online]. Available: https://www.cvedetails.com/cve/CVE-2017-5638/. [Accessed: 11-May-2019].

[16] “How to Stop the Next Equifax-Style Megabreach—Or At Least Slow It Down | WIRED.” [Online]. Available: https://www.wired.com/story/how-to-stop-breaches-equifax/. [Accessed: 19-Apr-2019].

[17] “Equifax hackers stole data for 200k credit cards from transaction history | Ars Technica.” [Online]. Available: https://arstechnica.com/information-technology/2017/09/equifax-hackers-stole-data-for-200k-credit-cards-from-transaction-history/. [Accessed: 19-Apr-2019].

[18] “Equifax breach disclosure would have failed Europe’s tough new rules | TechCrunch.” [Online]. Available: https://techcrunch.com/2017/09/08/equifax-breach-disclosure-would-have-failed-europes-tough-new-rules/?guccounter=1&guce_referrer_us=aHR0cHM6Ly9lbi53aWtpcGVkaWEub3JnLw&guce_referrer_cs=mVzWPa5UmuhNcT7pBYYemg. [Accessed: 19-Apr-2019].

[19] “Equifax Announces Cybersecurity Incident Involving Consumer Information -

DATAVERSITY.” [Online]. Available: https://www.dataversity.net/equifax-announces-cybersecurity-incident-involving-consumer-information/. [Accessed: 12-May-2019].

[20] “Personal Finance —Ep.29 - SOML: How I Protect My Credit After Equifax’s Data Breach — Dollars & $ense LA.” [Online]. Available: https://www.dollarsandsensela.com/blog/somlcreditbreach. [Accessed: 12-May-2019].

[21] “People are furious about the site Equifax set up to let you know whether your personal details were hacked - Business Insider Nordic.” [Online]. Available: https://nordic.businessinsider.com/equifax-data-breach-site-check-angry-response-2017-9. [Accessed: 19-Apr-2019].

[22] RepRisk, “REPRISK CASE STUDY Equifax Data Breach Scandal.”

[23] “All the Ways Equifax Epically Bungled Its Breach Response | WIRED.” [Online]. Available: https://www.wired.com/story/equifax-breach-response/. [Accessed: 12-May-2019].

[24] “One Year Later: The Impact of Equifax’s Data Breach | Transforming Data with Intelligence.” [Online]. Available: https://tdwi.org/articles/2018/10/29/biz-all-impact-of-equifax-data-breach.aspx. [Accessed: 12-May-2019].