A Case Study Analysis of the Equifax Data Breach 1 A Case Study Analysis of the Equifax Data Breach

Preprint · December 2019

DOI: 10.13140/RG.2.2.16468.76161

1 author:

Jason Thomas
American Military University
3 PUBLICATIONS **0** CITATIONS

SEE PROFILE

A Case Study Analysis of the Equifax Data Breach

Jason E. Thomas

A Case Study Analysis of the Equifax Data Breach

The Equifax data breach was one of the most significant cyberattacks of 2017. The attack's effects were far-reaching, affecting millions of people and multiple businesses and agencies. In fact, the attack was so concerning that the United States Government Accountability Office was engaged to investigate the incident and create a report for Congress about how to address the problem. This case study analysis will explore the facts and circumstances surrounding this damaging cyberattack, and critically analyze the factors concerning the case to draw conclusions about ways to mitigate future exposures. Lastly, a recent cyberattack will be explored along and a brief comparison of consumer susceptibility to cybercrime versus traditional crime.

Background

Equifax is one of the top three consumer credit reporting agencies. On September 8, 2017, Equifax released a statement that it had been a victim of a cyberattack resulting in a massive data breach (Fruhlinger, 2019; Rajna, 2018). The world was shocked to learn that in this data breach, some 148 million US citizens' sensitive personal data were compromised including names, dates of birth, Social Security numbers, and driver's license numbers (Marinos & Clements, 2018). In addition to personal information, some 209,000 credit card numbers were also stolen (Perez, 2017). The severity and scope of the Equifax data breach were unprecedented at the time. Though they had previously been larger breaches, the sensitivity and criticality of the personal identifying information in the financial information in this breach created a problem whose magnitude could barely be calculated at the time.

One of the issues that exacerbated the Equifax data breach was the fact that Equifax's main product is essentially derived from a database containing many of the US population's

personal and financial information. The data stored by Equifax contains each person's personal credit history, which includes personal identifying information, known addresses, and account numbers. Further, the system is not an *opt in* system, as the data is gathered from businesses rather than the individuals listed in the database. When a person borrows money, lending institutions report the information about payment history, balances, and other key information items. When someone wants to borrow money, the new lender checks this information to assess the borrowers credit risk, which is used to make a lending decision.

Factors That Contributed to the Breach

In the initial announcement, Equifax stated that miscreants had infiltrated their systems from May through July of 2017 (Gressin, 2017). The vulnerability that enabled miscreants to enter the Equifax systems and effect the data breach was a vulnerability called Apache Struts CVE-2017-5638. This vulnerability takes advantage of exception handling issues in the Jakarta Multipart parser of the software when users go to upload files. This vulnerability allows enables attackers from a remote location to execute arbitrary commands that can be created remotely by means of crafted: Content-Disposition, Content-Type, or Content-Length HTTP header with a Content-Type header containing the characters *#cmd=string* (NIST, 2018). Apache Struts is a popular framework for creating streamlined Java applications (The Apache Software Foundation, 2018). This useful product is used by many organizations, thereby making it an exceptional target for various cyber criminals because it can offer a potential entry point to a great number of victims and their information.

The Apache Software Foundation discovered the potential vulnerability and made a patch to correct it. Then they made an announcement to the world to inform them of the issue (Marinos & Clements, 2018). The patch was released on March 7, 2017. On March 8, 2017, the

Department of Homeland Security contacted Equifax as well as the other credit reporting agencies to notifying them of the system's vulnerability and directed them to install the patch. Equifax systems administrators were contacted on March 9, 2017 by the Apache Software Foundation, who also directed them to install the patch.

On March 15, 2017 some eight days after the patch announcement, seven days after notification from the Department of Homeland Security, and six days after notification from the vendor, Equifax conducted a scan of its systems (Marinos & Clements, 2018). The scanner report did not show a vulnerability to the Apache Struts issue. Consequently, the systems were unpatched and unprotected until July 29, 2017. During this time, the security department at Equifax noticed suspicious activity on the network. Equifax took the application off-line and three days and later hired an external cybersecurity firm to conduct a forensic investigation. The initial investigation indicated that many files were breached. Ultimately, this resulted in announcements that the personal information of some 145 million Americans, 8,000 Canadians, and 693,000 British citizens' information had been compromised due to a data breach.

External Responses to the Data Breach

Equifax's lackluster response to the notification of the vulnerability and bumbled handling of the notification of the breach was met with great criticism. Equifax had to create a separate domain and webpage to deal with all of the information that needed to be disseminated and to communicate with affected users and stakeholders (Equifax, 2019). This potentially well-intentioned business maneuver demonstrates the complexity of dealing with the issue. Other parties immediately initiated fake settlement sites and information sites creating additional opportunities for fraud and cybercrime as well as additional public confusion (Atleson, 2019). (Rajna, 2018)

Adding accident injury, the site was flagged as a phishing threat. Worse, Equifax customer service directed potential victims to one of the illicit phishing sites via their Twitter feed (Deahl & Carman, 2017). As customers flocked to freeze their credit reports, they were given PINs with naming conventions based on the date the accounts which were frozen. This unfortunately made them easy for cyberattackers to intuit and attack — enabling once again more potential and devastating attacks. Further, Equifax was criticized for offering free credit monitoring while trying to remove consumers' ability to sue them in the terms and conditions during the process to register for the service.

As the situation continued to worsen and spiral out of control, governments at virtually all levels begin to take notice and initiate inquiries and actions. Eventually, Equifax settled with all 50 State Attorney Generals in the United States for some $600 million (Oregon Department of Justice, 2019). The federal government also took notice. The Federal Trade Commission conducted an investigation and Congress held several hearings to investigate Equifax and bills were introduced in both the House and the Senate regarding business processes used by credit reporting agencies and privacy (Marinos & Clements, 2018).

Analysis of the Case

This data breach brought many glaring issues to light about Equifax's handling of the incident, the problems inherent with the credit reporting agencies, and the process of dealing with incident response. Consequently, there are many lessons to be learned from this historic cybercrime. These lessons will be discussed here.

Equifax Is Handling of the Incident

End-users are often cited as a primary vector for cyberattacks and cybersecurity experts often recommend aggressive user training and awareness as well as programs with adult oriented

training methodologies to prevent phishing attacks and identity theft (Jensen, Dinger, Wright, & Thatcher, 2017; Thomas J. E., 2018; Thomas & Hornsey, 2014). However, in this case, it seems the most significant contributing factors were systems management procedures. Specifically, the Equifax IT team did not apply the patch when it came out. Even after being prompted by multiple sources such as The Department of Homeland Security and the software vendor the IT department failed to apply the patch eliminating the vulnerability (Marinos & Clements, 2018).

It is been noted that the security team at Equifax conducted a scan to see if the vulnerability existed in the system (Marinos & Clements, 2018). It is also been reported that the scan did not detect the vulnerability Apache Struts CVE-2017-5638. This points to other potential IT systems management issues. One possibility is that the scanning software wasn't updated are properly patched do its list of current vulnerabilities did not contain the appropriate information to detect the vulnerability. As it is clearly known that the vulnerability did exist, another possibility is that the software used for scanning was ineffective or broken. However, it is more likely, in the author's opinion, that the scanning software wasn't updated and therefore was unable to the detect the vulnerability.

It also appears there is possible negligence on the part of the Equifax IT and security teams. Though a scan was conducted to see if the vulnerability was present. There specific guidance given on multiple occasions to apply the patch. Clearly the patch was not applied. Why did the team not simply look at the patches on the servers and verify that the patch was installed? In general, this is an easy process to perform in would've immediately indicated that the the patch was not applied.

From both an ethical and legal perspective a at management level, Equifax had a fiduciary duty to notify affected consumers that their information was compromised and to

attempt to remediate this situation. Equifax's handling of the situation can only be classified as subpar both before and after the incident. As stated above, Equifax's lack of patch management diligence and lackluster response to directives to apply the patch to address a known vulnerability was specifically responsible for the attack. Afterwards the firm seemed to act in a manner that was not consistent with quickly putting information about the attack or resolving the issue in an effective manner.

The firm tried to limit consumer's ability to seek legal redress and damges (Marinos & Clements, 2018) and three top-level executives sold some $1.8 million in company stock prior to the breach being disclosed publicly (Melin, 2017), presumably to not lose value on these large amount of stock shares. These actions certainly seem to indicate that there were potential profit motives inherent in the responses of Equifax and its executive team members. Executive incentives are commonly cited as motivators for executives to make decisions to preserve individual bonsu pay and company stock prices, rather than to preserve the interest of their customers or other stakeholders (Thomas J. E., 2017).

Problems Inherent with Credit Reporting Agencies

At the time of this attack there were many risks that were generated by the inherent nature with the credit reporting agency process for the United States. Consumers are involuntary members of the systems and did not and do not have the option to opt into the system, their information is reported by companies they do business with. This creates an unapproved and sometimes uninformed risk for most of the consumers in the United States. After the attack there was much discussion about the need to be able to freeze credit reports. Since then credit reports have moved from being able to be frozen for minor cost to being able to be frozen at no cost (Frost, 2018).

Government Response to the Incident

As previously discussed, governments at all major levels responded to the incident. Responses varied from chastising Equifax to seeking damages to creating new regulations regarding credit reporting agencies and privacy as well as specific sanctions against Equifax. In addition to heightened awareness and security, the federal government spearheaded two specific efforts to address future issues: an enhanced ability to freeze and unfreeze credit reports and detailed scrutiny about the need for data holders to notify consumers of data breaches (Deahl & Carman, 2017). One specific example of this is the passage of the Economic Growth, Regulatory Relief, and Consumer Protection Act (115th Congress, 2018).

Conclusion

At the time, the Equifax data breach was unprecedented and represented the largest most complex data breach known (Fruhlinger, 2019; Gressin, 2017; Marinos & Clements, 2018; Oregon Department of Justice, 2019). The breach was caused due to a known vulnerability that was published by the vendor and Equifax received several warnings to apply the patch that would prevent the vulnerability. However, enterprise systems management and cybersecurity is very complex and even though Equifax had a presumably large IT division, they were not able to use standard digital forensic techniques of systems management practices to identify and track the infiltration (Fruhlinger, 2019; Marinos & Clements, 2018; Thomas, Galligher, Thomas, & Galligher, 2019). The utilized an outside security firm to conduct forensics investigations. The simple act of failing to apply a patch and failing to check properly and to see if the patch was installed enabled a devastating cybercrime with far-reaching ramifications.

Due to the evolving nature of technology and its increasing use in daily life and business life new cybercrimes are being developed or committed on a frequent basis. These crimes range

from totally new technologies to committing types of cybercrimes to applying previous cybercrime methodologies to new targets as new technology is embraced. Cybercrime has become so prevalent, that many people are more worried about cybercrimes such as identity theft than home burglaries (hashedout, 2019). The complex nature and economies of scale for committing cybercrimes combined with the reduced cost and risk of executing the crimes make cybercrime the growingly popular choice of methology for committing criminal acts. Likewise. because of this vast array of methods and touch points – people are more susceptible to cybercrime than they are to traditional crimes.

References

115th Congress. (2018, May 24th). *S.2155 – Economic Growth, Regulatory Relief, and Consumer Protection Act.* Retrieved from Congress.gov: https://www.congress.gov/bill/115th-congress/senate-bill/2155

Atleson, M. (2019, July 2019). *Equifax data breach: beware of fake settlement sites.* Retrieved from Federal Trade Commission Consumer Information: https://www.consumer.ftc.gov/blog/2019/07/equifax-data-breach-beware-fake-settlement-websites

Deahl, D., & Carman, A. (2017, September 20). *for weeks, Equifax customer service has been directing victims to a fake phishing site.* Retrieved from the verge: https://www.theverge.com/2017/9/20/16339612/equifax-tweet-wrong-website-phishing-identity-monitoring

Equifax. (2019). *2017 cybersecurity incident & important consumer information.* Retrieved from equifaxsecurity2017.com: https://www.equifaxsecurity2017.com

Frost, A. (2018, September 6). *Equifax data breach: Still haven't frozen your credit since the huge hack? Here's how.* Retrieved from USA Today: https://www.usatoday.com/story/money/2018/09/06/equifax-data-breach-how-freeze-your-credit-report/1136955002/

Fruhlinger, J. (2019, October 14). *Equifax data breach FAQ: what happened, who was affected, was the impact?* Retrieved from CSO: https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html

Gressin, S. (2017, September 8). *The Equifax data breach: what to do*. Retrieved from The Federal Trade Commission Consumer Information: https://www.consumer.ftc.gov/blog/2017/09/equifax-data-breach-what-do

hashedout. (2019, November 14). *33 Alarming Cybercrime Statistics You Should Know in 2019.* Retrieved from Hashedout.com: https://www.thesslstore.com/blog/33-alarming-cybercrime-statistics-you-should-know/

Jensen, M. L., Dinger, M., Wright, R. T., & Thatcher, J. B. (2017). Training to mitigate phishing attacks using mindfulness techniques. *Journal of Management Information Systems, 34*(2), 597-626. doi:10.1080/07421222.2017.1334499

Marinos, N., & Clements, M. (2018, August). *Data Protection Actions Taken by Equifax and Federal Agencies in Response to the 2017 Breach*. Retrieved from Warren.senate.gov: https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf

Melin, A. (2017, September seven). *Three Equifax Manager Sold Stock before Cyber Hack Revealed.* Retrieved from Bloomberg: https://www.bloomberg.com/news/articles/2017-09-07/three-equifax-executives-sold-stock-before-revealing-cyber-hack

NIST. (2018, March 3). *CVE-2017-5638 Detail* . Retrieved from National vulnerability database: https://nvd.nist.gov/vuln/detail/CVE-2017-5638

Oregon Department of Justice. (2019, July 22). *50 State Attorney Secure 600 Million from Equifax in the Largest Data Breach Settlement in History.* Retrieved from Oregon Department of Justice: https://www.doj.state.or.us/media-home/news-media-releases/50-state-attorneys-general-secure-600-million-from-equifax-in-largest-data-breach-settlement-in-history/

Perez, L. (2017, September 8). *2019 Fed Meeting Predictions — A Fourth Fed Rate Cut Is Unlikely* . Retrieved from magnify money: https://www.magnifymoney.com/blog/news/freaked-equifax-hack-heres-need-know1475999910/

Rajna, G. (2018). Equifax Data Breach. *viXra*. Retrieved 12 7, 2019, from http://vixra.org/pdf/1808.0215v1.pdf

The Apache Software Foundation. (2018). *Apache Struts*. Retrieved from apachestruts.org: https://struts.apache.org/

Thomas, J. E. (2017). Lessons learned in management, marketing, sales, and finance incentive practices a decade after the Subprime Mortgage Crisis. *International Journal of Business and Management, 12*(3), 19-26. doi:10.5539/ijbm.v12n3p19

Thomas, J. E. (2018). Individual cyber security: Empowering employees to resist spear phishing to prevent identity theft and ransomware attacks. *International Journal of Business and Management, 13*(6), 1-24. doi:10.5539/ijbm.v13n6p1

Thomas, J. E., & Hornsey, P. E. (2014). Adding Rigor to classroom assessment techniuqes for non-traditional adult programs: A liifecycle improvement approach. *Journal of Instructional Research, 3*, 27-37. doi:10.9743/JIR.2014.3.20

Thomas, J., Galligher, R., Thomas, M., & Galligher, G. (2019). Enterprise Cybersecurity: Investigating and Detecting Ransomware Infections Using Digital Forensic Techniques. *Computer and Information Science, 12*(3), 72-80. doi:10.5539/cisv12n3p72