the Availability Digest

www.availabilitydigest.com
@availabilitydig

Equifax Hacked for Data on 143 Million Consumers

September 2017

One of the largest breaches in history of consumers' private financial data occurred in mid-2017. From May to July, the personal information of millions of individuals was stolen by hackers from Equifax. In addition, the hackers gained access to the credit-card information of a large number of cardholders.

While not the largest data breach in history, it may be the most damaging. It revealed personally identifiable information on nearly 100% of the U.S. workforce as well as consumers from other countries. Stolen were names, addresses, Social Security numbers, and dates of birth.

The hackers that breached Equifax's servers exploited a security vulnerability in Apache Struts.

Because of the magnitude of this hack, I was probably personally affected. In this article, I describe how the data breach was accomplished and what you can do to protect yourself. This is advice that I definitely plan to follow.

Equifax

Equifax is a credit-reporting agency. It collects information on more than 800 million consumers worldwide. It is the oldest of the three largest American credit agencies along with Experian and TransUnion.

The Breach

On July 29, 2017, Equifax's security team observed suspicious traffic accessing its web site. It blocked the traffic but noted continued unauthorized access the following day. Equifax took the affected web site offline and on August 2nd contracted with cybersecurity firm Mandiant to review the scope of the intrusion.

Mandiant determined that the hacking had begun in mid-May and that information concerning 143 million people had been obtained by the hackers. Names, addresses, Social Security numbers, birth dates, and in some cases driver's licenses had been obtained. In addition, credit-card numbers for 209,000 U.S. cardholders had been compromised. Information on some Canadian and U.K. consumers was also obtained.

The hacking was accomplished via a vulnerability in the Apache Struts application. Apache Struts is an open-source web application framework for developing Java-based web applications. The vulnerability was discovered and patched in mid-March, 2017.

Just days after the patch was released, cyber criminals attacked those who had failed to patch the exploit. Included in these attacks was Equifax. By the time the Equifax hack began in mid-May, Equifax had about

© 2017 Sombers Associates, Inc., and W. H. Highleyman
www.availabilitydigest.com
For discussion, contact editor@availabilitydigest.com

two months to apply the patch. Its failure to do so allowed hackers access to the Equifax database and led to the theft of information on millions of consumers.

Why didn't Equifax update its software when it became aware of the danger? Applying the patch was a labor-intensive task requiring the rebuilding of older, bug-plagued versions of Equifax. Consequently, Equifax delayed applying the patch.

Equifax believes that the unauthorized access occurred from May 13 through July 30, 2017, when it took its web site offline. Equifax has created a dedicated web site at www.equifaxsecurity2017.com, where consumers can understand whether they were affected by the hack and learn how to protect themselves.

How To Protect Yourself

If you are concerned that you may have been one of the consumers whose information was stolen, there are several steps you can take to protect yourself:

1.Check whether you were affected:

Equifax is providing a free tool that checks whether your information was part of the recent data breach.

2. Put a fraud alert on your credit report:

Ask one of the credit bureaus (Equifax, Experian, TransUnion) to put a fraud alert on your credit history. This will make it harder for anyone to impersonate you or affect your credit. You will also get a free copy of your credit report.

3. Review your credit report:

Scan your credit report to determine if there is any strange or suspicious activity.

4. Freeze your credit report:

Though this is a somewhat drastic step, it is a good way to ensure that no one else can impersonate you and ruin your credit score. You can unfreeze it at any time.

The Aftermath

The enormity of the Equifax hack had an immense impact on its market value, with its shares dropping 33% when it revealed the hack. This represented a $6 billion drop in its market capitalization.

The Federal Trade Commission and the Consumer Financial Protection Bureau have opened investigations into the hack.

Equifax Wasn't the Only One

It turns out that over 3,000 organizations downloaded the same Apache Struts module in the last twelve months. Additionally, almost 50,000 organizations downloaded versions of Struts with known vulnerabilities despite perfectly safe versions being available. Consequently, upwards of 50,000 organizations may be vulnerable to attack.

Summary

This is a painful example that teaches us that cyber resilience begins and ends with the Board of Directors and the senior executives of the company. It they had ensured that Equifax had applied the exploitation fix as soon as it became available, this hack would not have occurred.

From its annual reports, it is clear that customers, growth, shareholders, and investors mattered more to Equifax than managing cyber risk, privacy, or information security. In a keyword search through five years

© 2017 Sombers Associates, Inc., and W. H. Highleyman
www.availabilitydigest.com
For discussion, contact editor@availabilitydigest.com

of Equifax annual reports, researchers found terms such as risk management, cyber risk, privacy, data security, data breach, or information security that were barely mentioned. The other credit rating agencies, Experian and TransUnion, are somewhat more likely to mention privacy and risk management. One of the problems that these companies bring upon themselves is that risk management is treated as a cost center rather than as an imperative.

The CEO of Equifax will testify about the breach before Congress on October 3, 2017.

Acknowledgements

Information for this article was taken from the following sources:

Here's How to Protect Yourself from the Equifax Hack, *Popular Mechanics*; September 8, 2017.
Equifax Data Breach: Unpatched Apache Struts Vulnerability Was Exploited in Hack, *IB Times*; September 14, 2017.
The Kiplinger Letter, *Kiplinger*; September 15, 2017.
Equifax Had Patch, Didn't Install It, *USA Today*; September 15, 2017.
Equifax Releases Details on Cybersecurity Incident, Announces Personnel Changes, *Equifax*; September 15, 2017.
The Equifax Breach and 5 Years of Missed Warning Signs, *Huffington Post*; September 17, 2017.

© 2017 Sombers Associates, Inc., and W. H. Highleyman
www.availabilitydigest.com
For discussion, contact editor@availabilitydigest.com