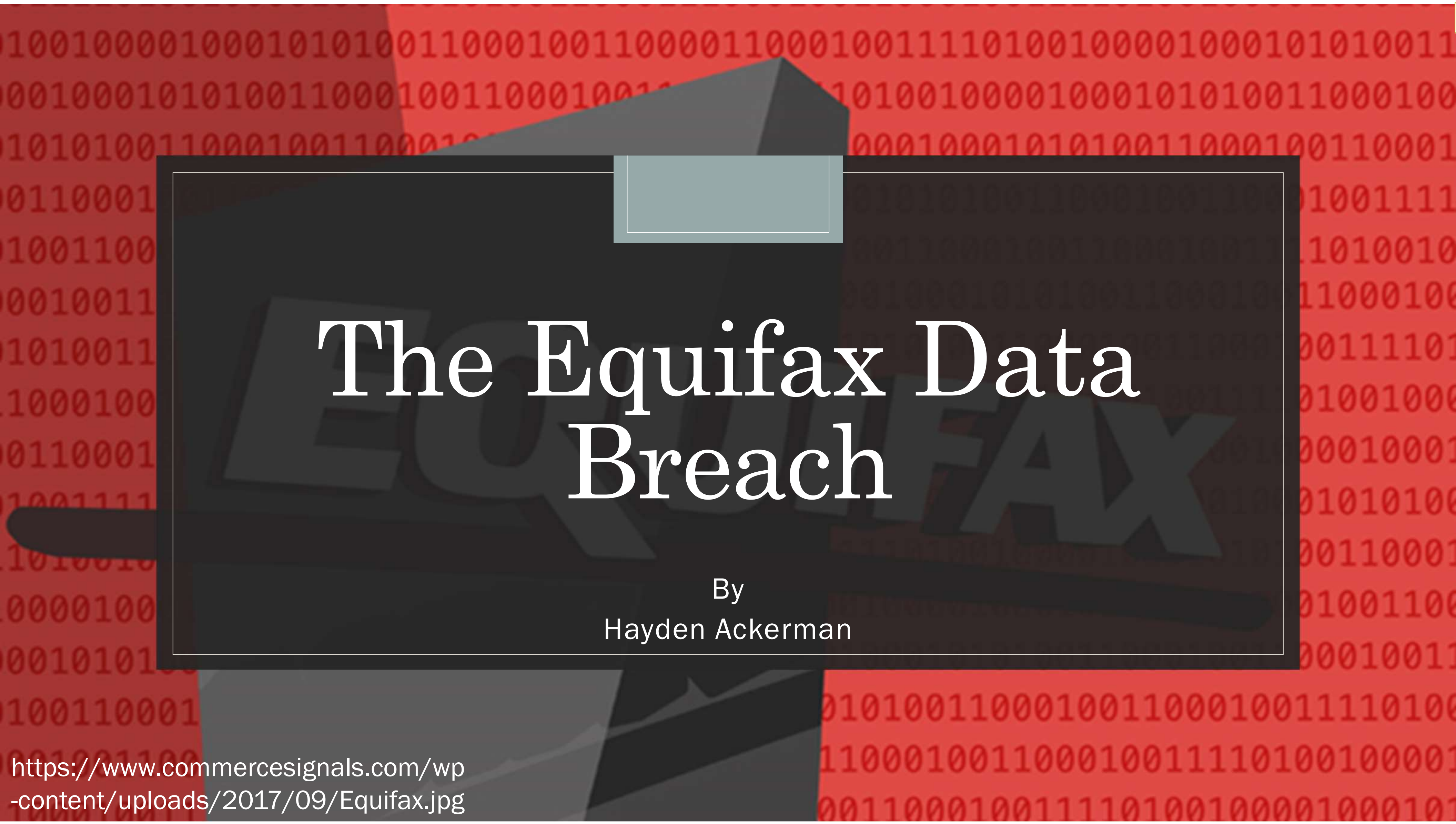


The Equifax Data Breach

By
Hayden Ackerman

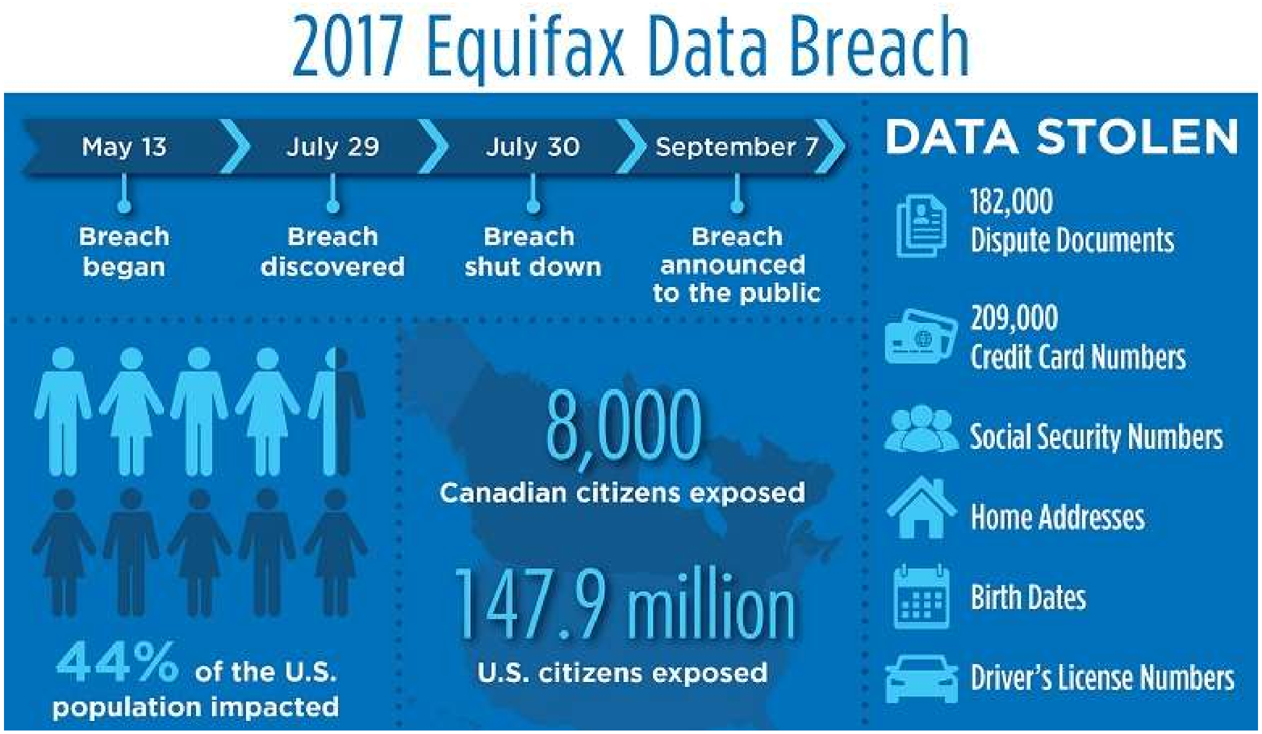
https://www.commercesignals.com/wp-content/uploads/2017/09/Equifax.jpg

Slide 1

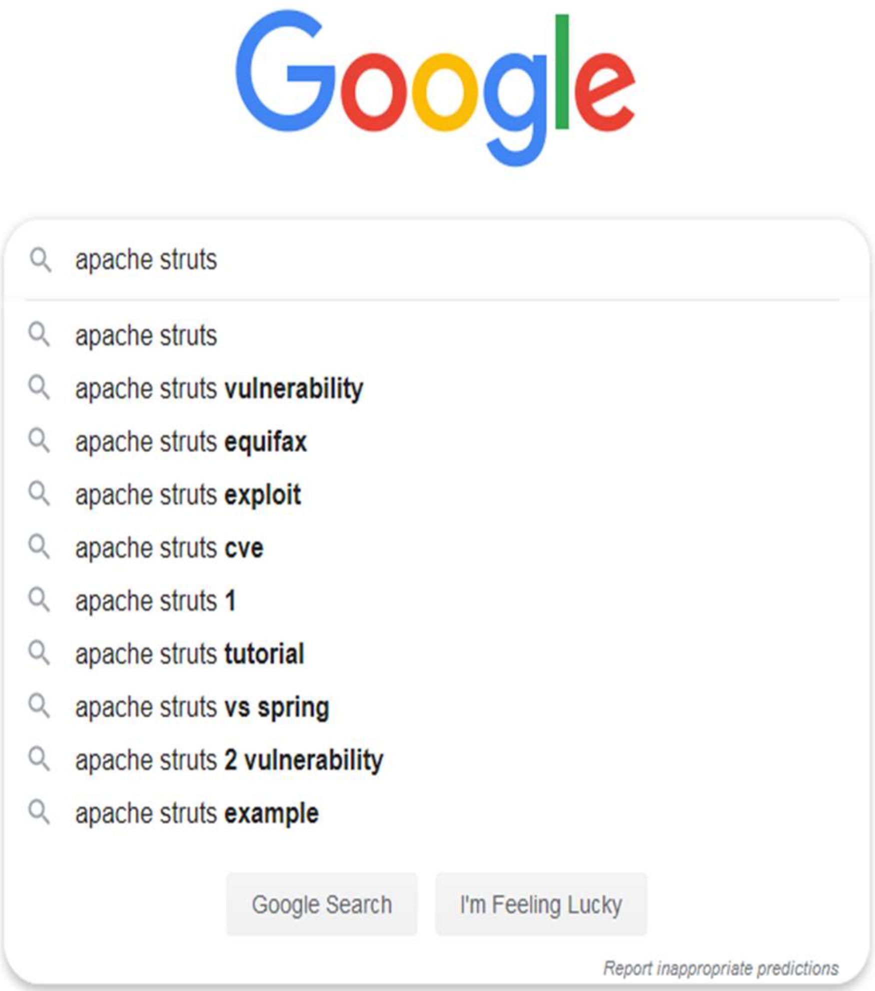
HA1 Hayden Ackerman, 11/29/2019

The Lowdown

- When: September 7, 2017. The breach was identified to have occurred on July 29, 2017.
- Where: Equifax, a massive consumer credit reporting agency.
- What: A data breach of *over* 150 million Americans personal info, including first & last names, SSNs, licenses, home addresses, phone numbers, and dates of birth.



https://www.alliedsolutions.net/-/media/alliedwww/images/equifax_infographic_r5_777x450.ashx?la=en&hash=28187C598E1B7BC0A64101E28E41CF3934E7CD7E



What Happened

It was a software issue. If one were to research Apache Struts, “vulnerabilities” would pop up in the search results more frequently than not.

Apache Struts is an open-source web app framework to create Java-based web applications.

Equifax was using an outdated version of Struts, which was vulnerable to an RCE (Remote Code Execution) bug. The bug, dubbed CVE-2017-5683. A patch was released on March 6-7 by the Apache Software Foundation.

Equifax was told to patch their systems but didn’t. In May, their systems were breached, and the exfiltration of data commenced until July of 2017, when they identified the breach and then patched their systems.

Attackers were unnoticed due to an expired public-key certificate causing the IDS (Intrusion Detection System) to fail.

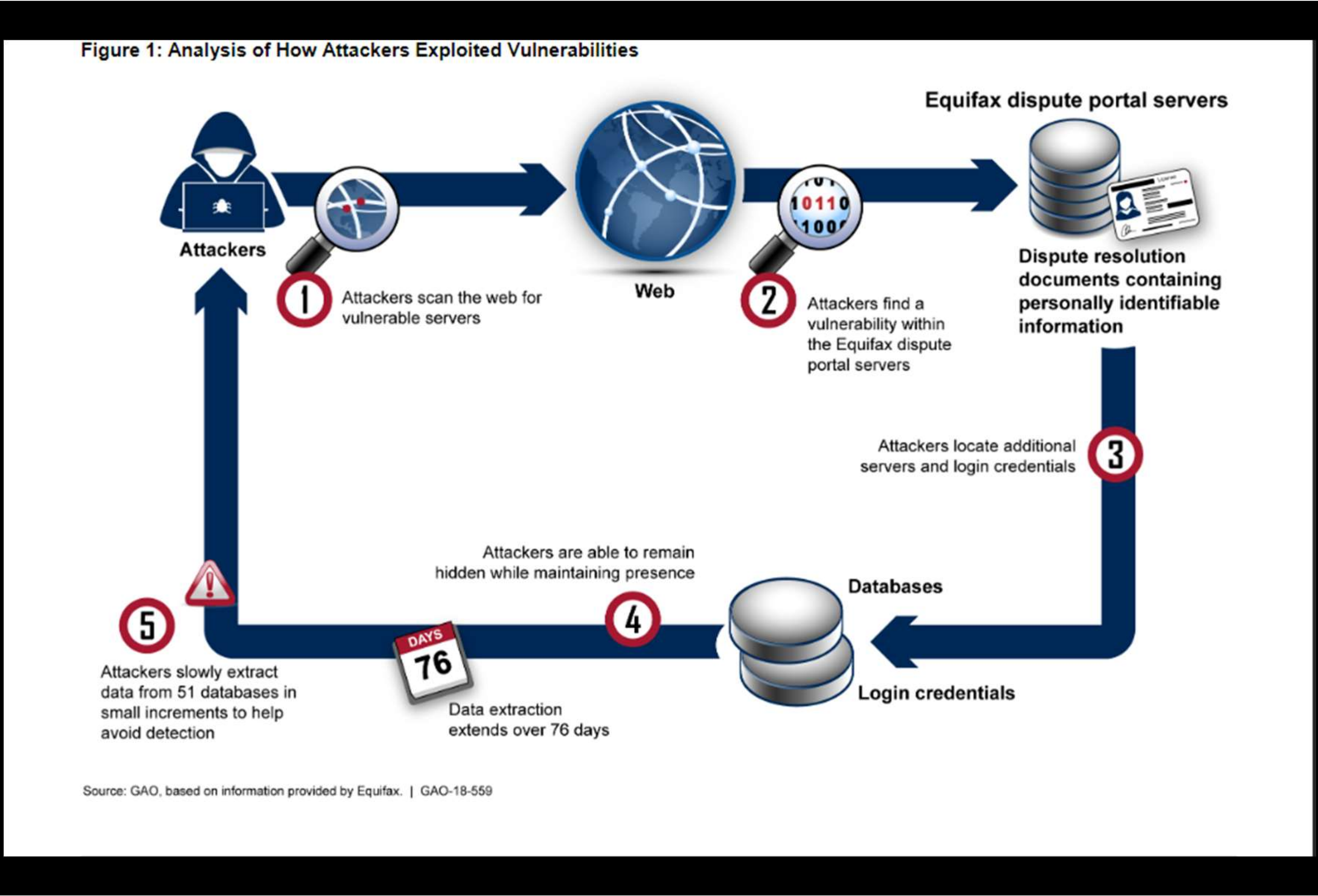


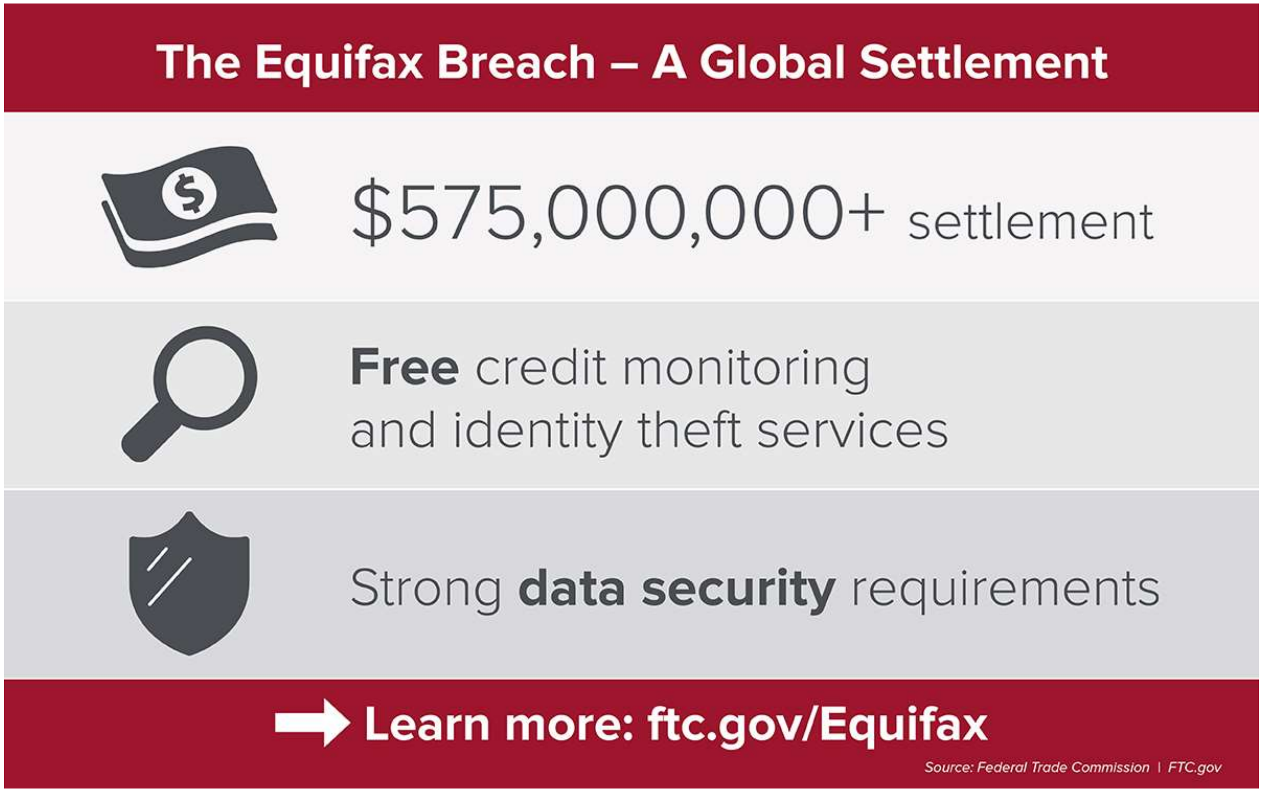
Figure 1: Analysis of How Attackers Exploited Vulnerabilities

Attackers
Web
Equifax dispute portal servers
Dispute resolution documents containing personally identifiable information
1 Attackers scan the web for vulnerable servers
10110
100
2 Attackers find a vulnerability within the Equifax dispute portal servers
3 Attackers locate additional servers and login credentials
Databases
Login credentials
4 Attackers are able to remain hidden while maintaining presence
DAYS
76
Data extraction extends over 76 days
5 Attackers slowly extract data from 51 databases in small increments to help avoid detection

Source: GAO, based on information provided by Equifax. | GAO-18-559

Damages & Reparations

- Financial: $1.4 billion + legal fees, due to numerous lawsuits.
- Consumer Trust: All time low.
- Reparations: Free credit monitoring, identity theft services, and a cash settlement option.



The Equifax Breach – A Global Settlement

$575,000,000+ settlement

Free credit monitoring and identity theft services

Strong **data security** requirements

➡ **Learn more: ftc.gov/Equifax**

Source: Federal Trade Commission | FTC.gov

Prevention

- Patch! Patch, patch, and patch some more! Equifax’s lackadaisical handling of their systems resulted in them being unpatched, therefore unprotected.
- Move away from Apache Struts. Struts is known to often have easily exploitable vulnerabilities. Look into the Spring Framework, Hibernate, etc.
- Don’t let expired certificates be your downfall! If Equifax had renewed the certificate for their IPS, they could’ve noticed the breach far sooner.
- Segment your systems! Equifax had too many systems connected.

Sources

- https://www.cnet.com/news/equifaxs-push-to-regain-public-trust-calls-for-companies-to-work-together/
- https://www.wabe.org/equifax-says-cybersecurity-breach-has-cost-1-4-billion/
- https://krebsonsecurity.com/2017/09/equifax-breach-response-turns-dumpster-fire/comment-page-3/
- https://www.consumer.ftc.gov/sites/www.consumer.ftc.gov/files/eqfx-socmed-summary.png
- https://www.csoonline.com/article/3444488/equifax-data-breach-faq-what-happened-who-was-affected-what-was-the-impact.html
- https://www.warren.senate.gov/imo/media/doc/2018.09.06%20GAO%20Equifax%20report.pdf
- https://cwiki.apache.org/confluence/display/WW/S2-057