Equifax breach was ‘entirely preventable’ had it used basic security measures, says House report

Zack Whittaker@zackwhittaker
Comment

A House Oversight Committee report out Monday has concluded that Equifax’s security practices and policies were sub-par and its systems were old and out-of-date, and bothering with basic security measures — like patching vulnerable systems — could’ve prevented its massive data breach last year.

It comes a little over a year after Equifax, one of the world’s largest credit rating agencies, confirmed its systems had fallen to hackers. Some 143 million consumers around the world were affected — most of which were in the U.S., but also Canada and the U.K. — with that figure later rising to 148 million consumers. Yet, to date, the company has faced almost no repercussions, despite a string of corporate failings that led to one of the largest data breaches in history.

The House report was scathing, criticizing the handling of the hack by Equifax’s former chief executive Richard Smith — who went on to “retire” following the breach.

Smith boasted that the credit giant held “almost 1,200 times” the data held in the Library of Congress every day, but the House report said that Equifax had “failed to implement an adequate security program to protect this sensitive data.”

“Such a breach was entirely preventable,” said the report.

The report confirmed most of what was already known, but added new color and insights that were previously unreported. The credit agency failed to patch a disclosed vulnerability in Apache Struts, a common open source web server, which Homeland Security had issued a warning about some months before. The unpatched Apache Struts server was powering its five-decades-old(!) web-facing system that allowed consumers to check their credit rating from the company’s website. The attackers used the vulnerability to pop a web shell on the server weeks later, and managed to retain access for more than two months, the House panel found, and were able to pivot through the company’s various systems by obtaining an unencrypted file of passwords on one

server, letting the hackers access more than 48 databases containing unencrypted consumer credit data.

During that time, the hackers sent more than 9,000 queries on the databases, downloading data on 265 separate occasions.

Equifax's former boss Smith passed the buck onto a single IT staffer for failing to patch the Struts system. In fact, it was just another example in the company's cavalier attitude toward data security, the House report found.

"Equifax did not see the data exfiltration because the device used to monitor [the vulnerable server's] network traffic had been inactive for 19 months due to an expired security certificate," the report said. It took another two months for Equifax to update the expired certificate, at which point staff "immediately noticed suspicious web traffic." Even Equifax's own former chief information officer David Webb — who also "retired" following the incident — told House investigators that the whole incident could have been prevented had the company updated the vulnerable Struts system within two days of the patch's release.

"Had the company taken action to address its observable security issues prior to this cyberattack, the data breach could have been prevented," said the report.

Two more months later, Equifax went public. That was no picnic either.

When Equifax's "are you at risk?" website wasn't crashing, it was spewing out incorrect results. Then the site was quickly impersonated — and was inadvertently linked to by Equifax's own social media staff. When concerned consumers finally got through to the site, they were offered Equifax's own credit freezing service, which was kicking out weak PIN numbers — the one and only thing that was protecting consumers' already fragile credit. The site was later pulled offline after another security researcher found a flaw in the credit freezing site that let an attacker siphon off sensitive consumer data. This was all while its call centers were overloaded, and many struggled to get basic questions answered.

In all, the House report didn't hold back its critique — slamming the credit rating agency's poor security practices, especially given the data involved — which the report noted that consumers do not "have the ability to opt out of this information collection process."

Equifax's response to the House's report? Go on the defensive.

“We are deeply disappointed that the Committee chose not to provide us with adequate time to review and respond to a 100-page report consisting of highly technical and important information,” said Equifax spokesperson Wyatt Jefferies. “During the few hours we were given to conduct a preliminary review we identified significant inaccuracies and disagree with many of the factual findings,” the statement continued.

“This is unfortunate and undermines our hope to assist the Committee in producing a credible and thorough public resource for those who wish to learn from our experience managing the 2017 cybersecurity incident,” the statement continued.

When TechCrunch asked for those “significant inaccuracies,” the spokesperson returned with a bulleted list of “factual errors” — or nit-picks — rather than pointing out substantial discrepancies with the report — including that Equifax offered two years of credit monitoring and not one year as was stated in the report, and that the report referenced an apparent settlement with a state attorney general that has not occurred.