GIZMODO

PRIVACY AND SECURITY

Equifax Is Finally Getting Kicked in the Money Bags Due to Its Disastrous 2017 Hack

Patrick Howell O'Neill
Yesterday 12:30pm

Mark Begor, CEO of Equifax, is sworn in during a Senate Homeland Security and Governmental Affairs Committee hearing on Capitol Hill, March 7, 2019 in Washington, DC. The committee heard testimony on investigations examining private sector data breaches.
Photo: Mark Wilson (Getty)

Two years ago exactly, someone began hacking Equifax. Today, it's starting to feel some pain.

The breach was made possible by a software vulnerability that was already known and fixable for months. The intrusion into Equifax's network began in May 2017 but wasn't discovered until July. The credit reporting company failed catastrophically to spot the data flowing out of its coffers. By the time anyone noticed, the information of about 150 million people was compromised, though it would take them several months to realize the full tally.

Congress has called the entire incident "entirely preventable" and one congressman called Equifax executives "stupid." Outside of Capitol Hill, the conversation was a lot less polite. Two years on, no one knows who stole that mountain of sensitive data or what they've done with it.

Wall Street is taking notice of the consequences. This week, the financial rating service Moody's downgraded Equifax from a "stable" to a "negative" outlook due to the high level of cybersecurity spending and litigation that comes as a direct result of the 2017 breach. It's the first time cybersecurity was cited as the reason for an outlook change, CNBC reported.

The numbers add up to a fortune, even for a massive corporation like Equifax. Lawsuits and investigations have cost $690 million in the first quarter of 2019 alone, which Moody's cited as one of the reasons for its outlook downgrade. Moody's expects $400 million more spent in each of the next two years and then a $250 million bill in 2021.

The cash Equifax will have to spend in relation to the cyberattack and bolstering its security are going to ding the company's profits, according to Moodys, which explained in its report that, after next year, Equifax's "infrastructure investments are likely to remain higher than they had been before the 2017 breach."

And the lawsuits will keep coming: In January, an Atlanta judge denied Equifax's attempts to dismiss class-actions filed against the company.

Equifax may be the first to have its outlook dinged as a result of a data breach but it is likely not the last.

"The heightened emphasis on cybersecurity for all data oriented companies, which is especially acute for Equifax, leads us to expect that higher cybersecurity costs will continue to hurt the company's profit and free cash flow for the foreseeable future," Moody's report said.

Many companies are spending more on cybersecurity. Equifax, however, is playing catch up and paying a premium to do so—although anyone hoping for a solid legislative solution would say the cash price Equifax is now paying is not nearly enough.

To drive home the point about Equifax's spectacular blunder, here are the highlights from a 2018 congressional report on the incident:

> **Entirely preventable.** Equifax failed to fully appreciate and mitigate its cybersecurity risks. Had the company taken action to address its observable security issues, the data breach could have been prevented.
>
> **Lack of accountability and management structure.** Equifax failed to implement clear lines of authority within their internal IT management structure, leading to an execution gap between IT policy development and operation. Ultimately, the gap restricted the company's ability to implement security initiatives in a comprehensive and timely manner.
>
> **Complex and outdated IT systems.** Equifax's aggressive growth strategy and accumulation of data resulted in a complex IT environment. Both the complexity and antiquated nature of Equifax's custom-built legacy systems made IT security especially challenging.
>
> **Failure to implement responsible security measurements.** Equifax allowed over 300 security certificates to expire, including 79 certificates for monitoring business critical domains. Failure to renew an expired digital certificate for 19 months left Equifax without visibility on the exfiltration of data during the time of the cyberattack.
>
> **Unprepared to support affected consumers.** After Equifax informed the public of the data breach, they were unprepared to identify, alert and support affected consumers. The breach website and call centers were immediately overwhelmed, resulting in affected consumers being unable to access information necessary to protect their identity.

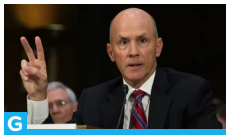
The cherry on top is the very nature of Equifax's business. There is an entire industry on which Equifax sits near the top that tracks every bit of personal data they can find about you. Credit reporting companies know about your bank accounts, credit card, date of birth, Social Security number, and much more.

Few people make an informed decision to hand all that data over to companies like Equifax which explains the surprise of many Americans when they found out their data was likely involved in that 2017 breach.

And if you are an American adult, the smart bet is that your data was stolen, too.

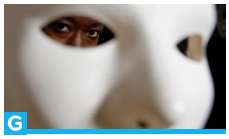
Oh Man, You're Gonna Hate What Equifax Just Admitted About That Security Breach

Report: Stolen Equifax Data Hasn't Been Sold Online, Raising More Questions Than Answers

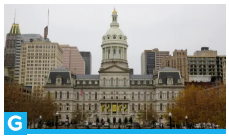


Equifax Breach Was Just as Infuriating and Dumb as You Thought, New House Report Finds

New Bill Would Require Agents to Actually Have Probable Cause to Search Electronic Devices at the Border



We Don't Need to 'Pause' Police Use of Face Recognition—We Need to Ban It Forever



Hackers Are Holding Baltimore's Government Computers Hostage, and It's Not Even Close to Over

ABOUT THE AUTHOR

Patrick Howell O'Neill

Patrick Howell O'Neill

Reporter in Silicon Valley. Contact me: Email poneill@gizmodo.com, Signal +1-650-488-7247

Fakes

Bullshit Viral Videos of Nancy Pelosi Show Fake Content Doesn't Have to Be a Deepfake

Matt Novak
May 24, 2019

1.5K 4 1

Two videos of House Speaker Nancy Pelosi have gone viral over the past 24 hours, raising ethical questions about the use of editing on social media. President Donald Trump even shared one of the videos last night, calling it "PELOSI STAMMERS THROUGH NEWS CONFERENCE." But only one of the videos is truly "fake" and surpri...

See More

Yesterday 4:35pm

Wikileaks Founder Julian Assange Charged With Espionage by U.S.

Dell Cameron
Yesterday 4:35pm

24 Save

Yesterday 7:00pm

The FDA Tells the Food Industry to Change How It Uses 'Expiration' Dates

Ed Cara
Yesterday 7:00pm

152 Save

Yesterday 6:45pm

Uber and Lyft Drivers Strike Alongside Fast Food Workers in LA, Demand $30 Minimum Wage

Bryan Menegus
Yesterday 6:45pm

283 Save