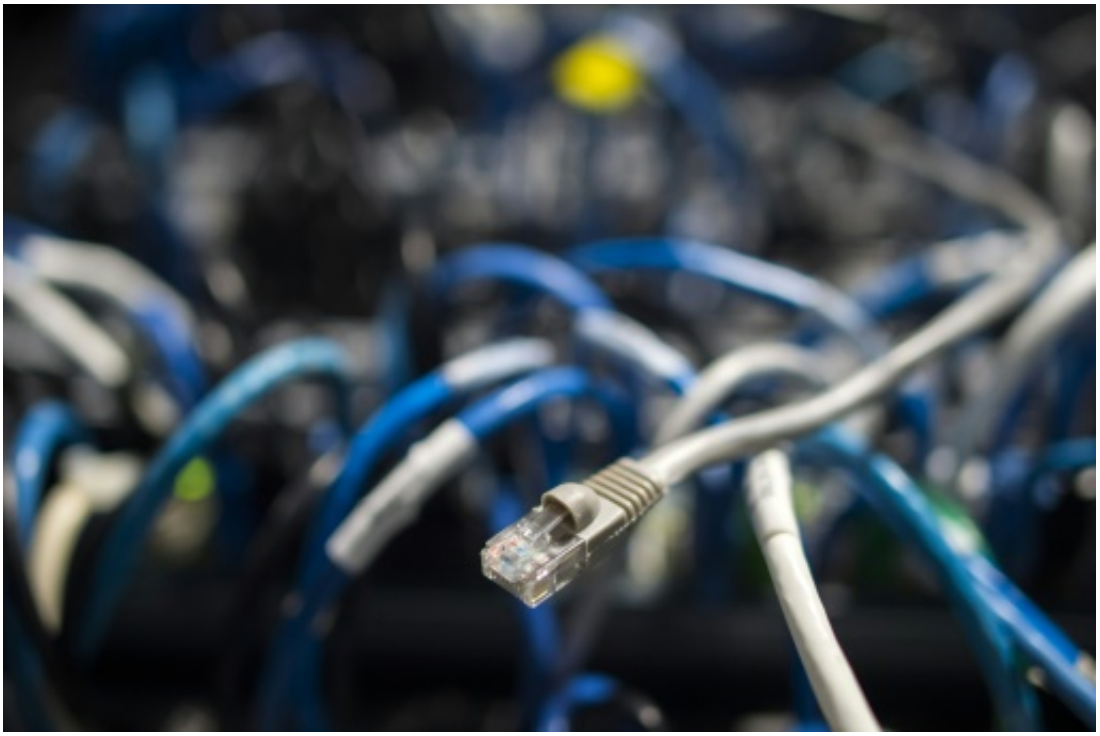
Massive credit bureau hack raises troubling questions

September 9 2017



The Equifax data breach is not the largest on record but could be the most damaging because of the sensitive nature of the information held by the credit reporting agency

It could be the worst-ever data breach for American consumers, exposing some of the most sensitive data for a vast number of US households.

The hack disclosed this week at Equifax, one of the three major credit bureaus which collect consumer financial data, potentially affects 143 million US customers, or more than half the adult population.

While not the largest breach—Yahoo attacks leaked data on as many as one billion accounts—the Equifax incident could be the most damaging because of the nature of data collected: bank and social security numbers and personal information of value to hackers and others.

"This is the data that every hacker wants to steal your identity and compromise your accounts," said Darren Hayes, a Pace University professor specializing in digital forensics and cybersecurity.

"It's not like the Yahoo breach where you could reset your password. Your information is gone. There's nothing to reset."

Some reports suggested Equifax data was being sold on "dark web" marketplaces, but analysts said it was too soon to know who was behind the attack and the motivation.

"This could be a mercenary group or it could be a nation-state compiling it with other data" for espionage purposes, said James Scott, a senior fellow at the Institute for Critical Infrastructure Technology, a Washington think tank.

"This is the kind of information I would go after if I were a nation-state, to set up psychographic targeting for information and political warfare."

National security risks

Peter Levin, chief executive at the data security firm Amida Technology Solutions and a former federal cybersecurity official, said he is concerned over the national security impact of the breach, which follows

a leak of data on millions of US government employees disclosed in 2015.

"The implications with regard to national security are very large," he said.

Because most federal employees also have credit reports, "those people have now been hacked twice," Levin said, offering potential adversaries fresh data to be used against them.

"We've just given the bad guys a lot more information," he said. "Even if they didn't perpetrate the attack, they can buy the data."

An FBI statement said the US law enforcement agency "is aware of the reporting and tracking the situation as appropriate."

The breach raised numerous questions among experts, such as why the company waited more than a month to notify consumers after learning of the attacks July 29.

Some analysts expressed concern that a company with a mission to safeguard sensitive data allowed a breach of this scope to take place.

"Equifax knew it was a prime target for cyberattacks," said Annie Anton, who chairs the Georgia Tech School of Interactive Computing and specializes in computer security research.

"It's amazing that one flaw could lead to a breach involving 140 million people. They should have safeguards in place. Even if a breach happens, it shouldn't grow to that scale."

Even more surprising, Anton said, is that Equifax still used social security numbers for verification despite the known risks from storing

these key identifiers.

Anton noted that she testified before Congress in 2007 recommending that credit bureaus be required to use alternatives to social security numbers "and it still hasn't been fixed."

Some details of the attack remain unclear, including whether the data stolen was encrypted—which would make it harder for the hackers to monetize.

At least two class-action lawsuits on behalf of consumers were filed following the disclosure claiming Equifax failed to adequately protect important data.

Equifax "should have been better prepared for any attempt to penetrate its systems," said attorney John Yanchunis, who filed one of the lawsuits.

Separate lawsuits announced Friday meanwhile said Equifax may have violated securities laws by allowing three high-ranking Equifax executives to sell shares worth almost $1.8 million in the days after the hack was discovered.

An Equifax spokesperson told AFP the executives "had no knowledge that an intrusion had occurred at the time they sold their shares."

Equifax stock fell 13.6 percent in New York trades on Friday following the disclosure.

- How to respond-

The potential impact of the Equifax breach prompted some experts to suggest the government revisit the idea of social security numbers issued for life.

"The government should consider changing social security numbers since there have been so many breaches," Hayes said.

Levin added that he "would be in favor of issuing new social security," even though "it's a fraught political discussion."

Others said the US could follow a European rule set to take effect in 2018 requiring companies to notify consumers within 72 hours of a data breach.

"Companies will put more into cybersecurity if there are tough penalties associated with data breaches," Hayes said.

The House Financial Services Committee will hold hearings on the breach, committee chair Jeb Hensarling said while expressing concern over a "very troubling situation."

New York state attorney general Eric Schneiderman said his office was launching a formal probe to determine if Equifax adequately notified consumers and had appropriate safeguards in place.

Citation: Massive credit bureau hack raises troubling questions (2017, September 9) retrieved 26 June 2024 from https://phys.org/news/2017-09-massive-credit-bureau-hack.html