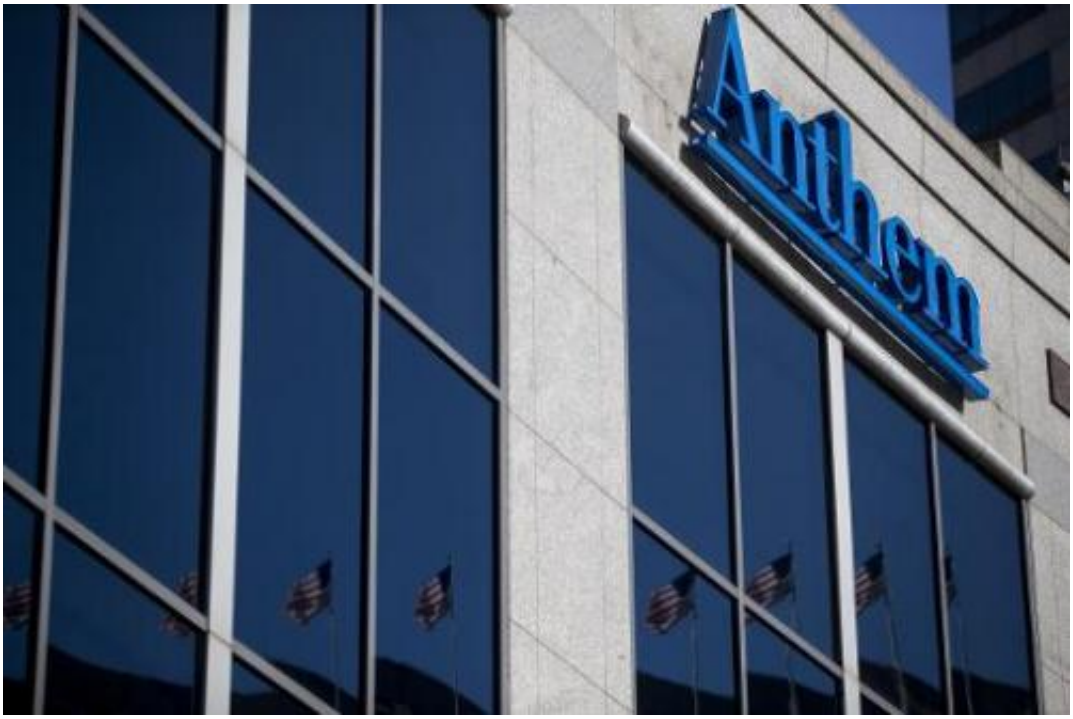
Giant US health-data breach could lead to China

February 5 2015



Data on as many as 80 million customers at US health insurance giant Anthem was stolen by hackers, officials confirm

Data on as many as 80 million customers at US health insurance giant Anthem was stolen by hackers, officials confirmed Thursday, in a cyberattack investigators have reportedly linked to China.

The Bloomberg News agency cited three people with knowledge of

Anthem's investigation as saying that cybersleuths believed the breach bore the hallmarks of previous attacks blamed on Chinese hackers.

The cyberattack is just the latest exposing personal information on millions of people in the United States, triggering calls for companies to beef up their data defenses.

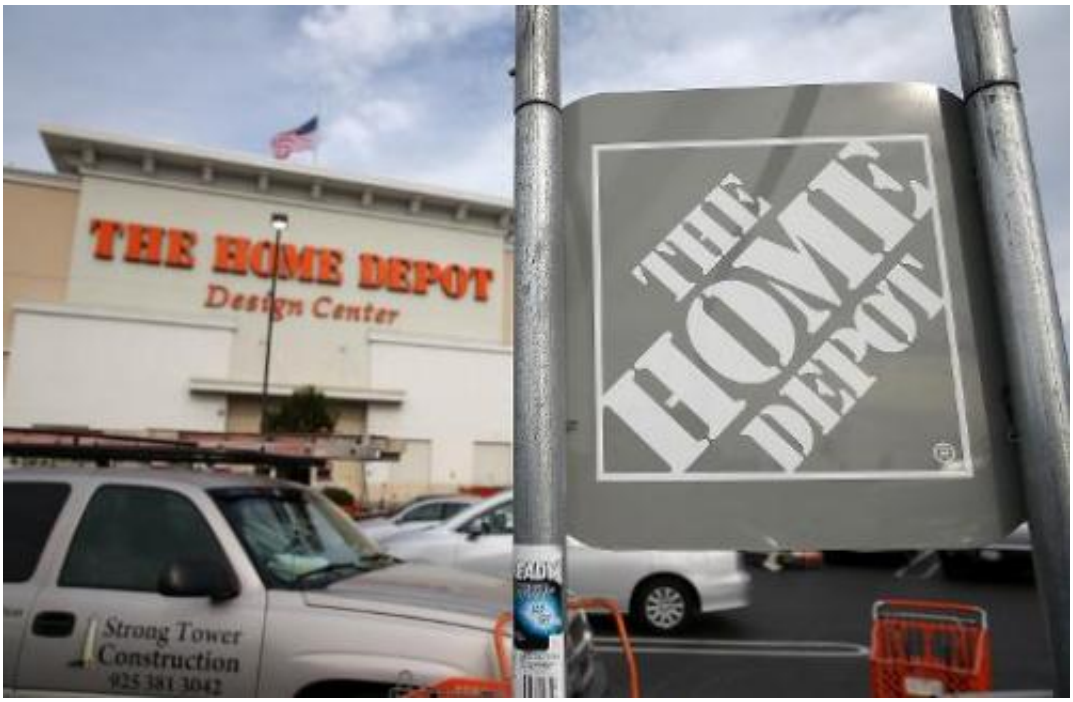
"Cyberattackers executed a very sophisticated attack to gain unauthorized access to one of Anthem's IT systems and have obtained personal information relating to consumers and Anthem employees who are currently covered, or who have received coverage in the past," a statement from the second-largest US health insurer said.

"Once the attack was discovered, Anthem immediately made every effort to close the security vulnerability, contacted the FBI and began fully cooperating with their investigation," said chief executive Joseph Swedish.

"Anthem's own associates' personal information—including my own—was accessed during this security breach. We join you in your concern and frustration, and I assure you that we are working around the clock to do everything we can to further secure your data."

The information includes names, birth dates, social security numbers, street addresses, email addresses and employment information, the company said.

"The affected database has records for 80 million people and tens of millions" of them were stolen, spokeswoman Cindy Wakefield said.



Last year, US retailer Home Depot said 53 million email addresses were stolen

China link

Bloomberg and The Wall Street Journal reported that while the investigation into the attack was nascent, there were indications it could be part of a broader spying campaign instead of profit-driven identity theft.

With details about a person's medical records, for example, cyber spies could craft emails that appear legitimate but are rigged with malicious software to gain access into networks of businesses or government agencies where they work.

Last year, US retailer Home Depot said 53 million email addresses were stolen, months after fellow retailer Target said personal data on 70 million customers was accessed.

Some experts say medical data can be even more lucrative to hackers than credit cards because they can create fake identities for prescription drugs to be resold, or file false insurance claims.

Security experts welcomed Anthem's decision to make the issue public swiftly.

"I'm pleased to see Anthem publishing information about the security breach online, and I'm sure customers will be grateful that the company has not tried to hide away the news," independent security researcher Graham Cluley said in a blog post.

"But what's really necessary is for companies and organizations to do a better job at protecting our personal information. Too many firms who are entrusted with data from the general public are finding themselves in the uncomfortable position of admitting that they have been hacked."

The United States government has long accused China of mounting an aggressive cyberwar against American companies and interests, charges routinely denied by Beijing.

FBI director James Comey last October said China was at the "top of the list" of countries launching cyberattacks on US firms.

"There are two kinds of big companies in the United States," Comey said. "There are those who've been hacked by the Chinese and those who don't know they've been hacked by the Chinese."