Cybersecurity breach rocks Anthem

James J. Giszczak, Dominic A. Paluzzi, Miriam L. Rosen | Thursday, February 5, 2015

In what may potentially be the largest data breach of a healthcare company, Anthem, Inc., the country's second-largest health insurer announced that it was the target of the latest big breach. Not only may this be the biggest data breach for the healthcare industry, it may also be one of the largest involving consumer information.

On February 4, 2015, Anthem disclosed that hackers had breached its computer system, which extended across all of Anthem's businesses, and infiltrated a database containing information on as many as 80 million members who are currently covered or who have received coverage, including its chief executive. Anthem has 37 million members in 14 states, but warned that information in the infiltrated database included Blue Cross Blue Shield patients from all 50 states who had sought care in its coverage area. Anthem is describing the attack as "a very sophisticated external cyber attack," but it is still unclear how exactly the attack was executed.

Breach discovered on January 27

Investigators are still determining the full extent of the breach, which Anthem first discovered on January 27, 2015. After the company's internal investigation, Anthem confirmed the cyberattack, and believes the unauthorized access to the database goes back to December 20, 2014. According to CNN Money, Anthem said it is likely that "tens of millions" of records were stolen, exposing names, dates of birth, addresses, member ID numbers, phone numbers, email addresses, Social Security numbers, and employment

information. While some of the member data may also include income information, at this point the breach does not appear to involve medical or financial information, such as credit card or bank account information.

While there is never a good time for a data breach, the timing could not have been worse for Anthem, as they are currently working on signing up thousands of people in Affordable Care Act coverage before the February 15th deadline.

Anthem's response plan

Anthem's response to the breach included promptly notifying the FBI of suspicious network activity. In these situations, a company's ability to quickly and effectively respond to a breach is critical because hackers can quickly destroy critical evidence necessary to determine the guilty party. As part of its response, Anthem has established a website and a toll-free number for member questions. While some Anthem customers received an email notification about the incident on February 4, 2015, from Anthem's CEO, the company said it would begin notifying others in the coming weeks through written notification in the mail.

Takeaways

The last year has been littered with an increasing number of sophisticated cyber hacks — each new one seemingly competing against the last to be the biggest and the most severe. Although the retail (Staples, Target, and Home Depot), financial (JPMorgan Chase), and entertainment (Sony) industries have already been significantly impacted, this Anthem breach is potentially the biggest one to hit the healthcare industry to date.

As the number of cyberattacks continues to rise and fill our newsfeeds, it is no wonder the FBI now puts cybercrime as one of its top law enforcement activities, according to *The New York Times*. This also explains why President Obama recently proposed a new law, which includes dramatically increasing spending on cybersecurity to $14 billion.

Do you have a response plan?

For companies large and small, this breach is yet another reminder of the importance of having a response plan in place prior to a breach. Proactive measures, like putting together a response plan and conducting exercises with key players to ensure everyone understands their role, are imperative for a company to quickly and effectively respond to a breach. Unfortunately, it now seems that it is no longer a matter of whether a company will be hacked, but when it will be hacked. Faced with this reality, your next steps are clear: **Be vigilant. Be prepared.**

Suggestions for individuals affected by the Anthem breach

For potentially impacted individuals, the following are some suggestions of what you can do to further protect yourself from the potential adverse effects of this type of data breach:

- Place a fraud alert on your credit account with one of the major credit monitoring companies (Equifax, TransUnion or Experian).
- Consider placing a security freeze on your credit files.
- Always remain vigilant in reviewing your financial account statements for fraudulent or irregular activity on a regular basis.
- Do not respond to any emails or phone calls asking for any of your personally identifiable information

or health information.

For more information, please contact one of the attorneys listed below.

James J. Giszczak

Team member bio

Dominic A. Paluzzi

Team member bio

Miriam L. Rosen

Team member bio