

<http://www.computerworld.com/action/article.do?articleId=296490&command=viewArticleBasic>

Pfizer Breach Illustrates Risks of Sharing Files

Personal data of 17,000 employees exposed via P2P application on laptop

Jaikumar Vijayan [Today's Top Stories](#) ▸ or [Other Security Stories](#) ▸



[Comments \(1\)](#) Recommendations: **86** — [Recommend this article](#)

June 18, 2007 ([Computerworld](#)) --

Pfizer Inc. disclosed this month that the Social Security numbers and other personal data of about 17,000 of its current and former workers were exposed after an employee installed unauthorized file-sharing software on a company laptop provided for use at her home.

Data on about 15,700 of the workers was actually accessed and copied off of the laptop by an unknown number of people on a peer-to-peer (P2P) network, New York-based Pfizer said in letters that it sent to affected employees and to state attorneys general.

Pfizer officials didn't respond to a request for comment last week. But copies of the pharmaceutical company's letters were posted on the Web site of the New Hampshire attorney general's office, and the office of Connecticut Attorney General Richard Blumenthal posted a response that he sent to a Pfizer attorney on June 6.

In his letter, Blumenthal noted that 305 Connecticut residents were among the affected employees. He asked the company to provide additional information by this Friday, including when it discovered the breach, how it responded and what kind of measures it had in place prior to the breach to protect against data compromises (see box).

The letter that Pfizer sent to the 17,000 individuals — which was dated June 1 and signed by Lisa Goldman, its general counsel — didn't specify when the file-sharing software was installed on the laptop or how the company discovered the data breach. But the letter did say that Pfizer reclaimed the laptop and disabled the file-sharing program immediately after discovering the breach. Goldman added that because the laptop was being used to access the Internet from outside of Pfizer's network, no other data was compromised.

Stark Example

The incident at Pfizer serves as a stark example of the potential security dangers presented by peer-to-peer software — dangers that were highlighted in a report released June 4 by Dartmouth College's Tuck School of Business.

The report was based on searches of P2P networks such as Gnutella, FastTrack, eDonkey and BitTorrent for traffic that mentioned the names of the top 30 U.S. banks or mapped to a specific digital footprint that Dartmouth created for each bank.

The data, which was gathered during a seven-week period from December to February, showed that a large number of people were inadvertently exposing bank account data and other personal information stored on their computers to fellow users on the P2P networks, said Eric Johnson, a professor of operations management at Tuck's Center for Digital Strategies.

Johnson, the report's author, said the data gathered also indicated that cybercrooks were lurking on P2P networks to harvest the financial data of users via targeted searches.

Data can be exposed in several ways, said Johnson. For instance, if a music file is accidentally dropped into a folder containing sensitive data, the entire folder could end up being made available on a P2P network without the user's knowledge, via wizards in file-sharing clients that can scan PCs and recommend folders containing media files for sharing.

"In many cases, [P2P users] are sharing the contents of their entire hard drive, with all sorts of information," Johnson said. And it isn't just home users who are at risk, he added. About 20% of the data analyzed in the Dartmouth study came from users at banks or their partners, Johnson said