

# Understanding Data Security Risks of P2P

By Brian Prince  
2008-04-25

Article Views: 1313  
Article Rating: ★★★★★ / 5

## Table of Contents:

1. Understanding Data Security Risks of P2P
2. Blocking Is a Simple Answer, but Difficult Solution

## Understanding Data Security Risks of P2P ( Page 1 of 2 )

### **Companies face unexpected risk of data loss from employees using peer-to-peer networks.**

Peer-to-peer file transfers are increasingly a source of data leaks, and IT organizations may not be appreciating the risk.

According to a survey by the Ponemon Institute of 750 IT professionals released the week of April 21, although 63 percent of respondents said their organizations forbid the use of P2P applications, only 5 percent said their organizations monitor P2P networks for data leaks. Twenty-six percent admitted they were unaware of any policies regarding P2P applications.

The problem was underscored in 2007 when a former employee of Citigroup's ABN AMRO mortgage group leaked the personal information of 5,000 people via a P2P messaging network. Pharmaceutical giant Pfizer also experienced a breach courtesy of a P2P application that exposed the personal data of 17,000 people.

### **Cyber-criminals use P2P tools for identity theft, a security analyst warns. [Click here to read more.](#)**

Tiversa, which sponsored the study and monitors P2P networks, reported that the previous week it had uncovered W2 forms for 2,498 employees of a company coming from that company's own network. The user in that case was on the Gnutella network using LimeWire, and while the organization had a policy against P2P usage, the employee disregarded it, said Robert Boback, CEO of Tiversa. Adding to the issue is that peer-to-peer networks are typically designed to circumvent firewalls and go over Port 80 instead of other monitored ports, he said.

"Our research shows that the highest time of use is during the U.S. work day—these aren't kids downloading files at night; P2P users are often individuals at work taking advantage of their high bandwidth," Boback said. "For many companies that have put security measures in place, we still find files disclosed from their internal corporate IP range because P2P is very good at getting around IT measures."

In addition, files coming across P2P can be disguised to look like legitimate MP3s but instead be Trojans. Paula Skokowski, vice president of marketing at secure file transfer vendor Accellion, said spyware and viruses transmitted via P2P file sharing can spread very rapidly and widely among users.

**Understanding Data Security Risks of P2P - Blocking Is a Simple Answer, but Difficult Solution**  
( Page 2 of 2 )

There is of course a simple answer to the problem—block P2P applications. However, Gartner analyst Peter Firstbrook noted that it is not easy to block all of them, and users actively look for ways to avoid the blocks, such as using laptops when they are out of the network. In addition, data loss prevention tools are not widely deployed, he said.

"[DLP tools] are mostly just monitoring versus blocking to avoid blocking legit business, so it is a bit like [closing] the proverbial barn door after the horse," Firstbrook said. "A well-configured DLP solution should catch P2P leaks, but that is not deployed in most organizations."

For companies, anywhere from 40 to 60 percent of the confidential files disclosed on P2P file-sharing networks originate from sources outside the corporate perimeter, such as suppliers, contractors, attorneys, partners, and employees working from home or on the road, Boback said.

"These endpoints are almost impossible for a company to control," he said, referring to those third-party sources as the extended enterprise. "An organization must take an extended enterprise view because very often the information custody chain extends outside their four-walled perimeter security approaches."

[Email Article To Friend](#) ♦ [Print Version Of Article](#) ♦ [PDF Version Of Article](#)

Print Version Sponsored By

[Email Article To Friend](#) ♦ [Print Version Of Article](#) ♦ [PDF Version Of Article](#)

Print Version Sponsored By