

Beware P2P Networks With A Tunnel To Confidential Data, Study Warns

Many of the biggest breaches in recent years were inadvertent disclosures, Dartmouth business school researchers found.

By Larry Greenemeier, [InformationWeek](#)

May 15, 2007

URL: <http://www.informationweek.com/story/showArticle.jhtml?articleID=199600527>

[Peer-to-peer networks](#) could be more than a nuisance in the workplace, they might also be providing cyberthieves with a tunnel into your most confidential data. So says a new study of [corporate data leaks](#) released Tuesday by Dartmouth business school researchers.

"Many of the biggest breaches in recent years were inadvertent disclosures," says Eric Johnson, professor of operations management at Dartmouth's Tuck School of Business and director of the school's Glassmeyer/McNamee Center for Digital Strategies. Johnson co-authored the study along with Scott Dynes, a senior research fellow at Dartmouth's Institute for Security Technology Studies.

One of the major problems, they found, was that users were insufficiently protecting their files and data from peer-to-peer networks. "Like most people I talked to, I underestimated the scope of the problem," Johnson told *InformationWeek*. "The kinds of leaks coming out of these organizations would make their hair stand on end, in terms of both the amount and type of information leaked."

The Dartmouth study notes that there are an estimated 10 million users sharing music, video, software, and photos over peer-to-peer networks, up from about 4 million in 2003. This doesn't even include [BitTorrent](#), a popular peer-to-peer application for video files that's difficult to monitor. Meanwhile, efforts by ISPs, corporations, and copyright holders to limit peer-to-peer through technology (such as site blocking, traffic filtering, and content poisoning) or through the courts (the most notable being the [Recording Industry Association of America](#) prosecution of individual users and file sharing firms) have prompted peer-to-peer developers to create decentralized, encrypted, anonymous networks that can find their way through corporate and residential firewalls.

"These networks are almost impossible to track, are designed to accommodate large numbers of clients, and are capable of transferring vast amounts of data," the study says.

And now the bad news. Criminals are actively searching peer-to-peer networks for any personal information they can use to [commit identity theft](#). There are several ways for confidential data to find its way to a peer network, including instances where users accidentally share folders containing such data, users store music and other data in the same folder that is shared, or users download malware that exposes their file directories to the network. A lot of identity theft victims "don't realize that their son was on [LimeWire](#) last night sharing their financial information," Johnson says. "Much of this software has interface designs that are confusing and even deceptive in a way that gets people to share, without knowing it, their whole hard drive."

Identity theft has become a bleak fact of life for many people. Many would-be identity thieves simply troll the Internet looking for sensitive information mistakenly posted to Web sites. Johnson and his colleagues have tracked this behavior by ordering

credit cards and phone cards and then publicly disclosing account information via the Web. "We leaked a live Visa card so we could watch what the thieves were doing with the information," he says, adding that he found that cyberthieves were using the stolen accounts in conjunction with PayPal and other online payment services to try to cover their tracks.

Johnson and his colleagues found lots of supposedly confidential information floating freely out on the Web, including job performance reviews and a bank's spreadsheet containing 23,000 business accounts including their contact names and addresses, account numbers, company positions, and relationship managers at the bank. He even found the results of a "confidential" security audit that a company had commissioned. Whoops.

One of the most effective ways to prevent business information from being leaked through peer-to-peer networks is to understand how these services are used. "Security people say they've blocked ports inside their firewalls so that users can't connect into peer-to-peer networks," Johnson says. "That's fine until those employees take their laptops home at night or go to a Starbucks and connect to a peer-to-peer network."

There are ways of tracking whether corporate data has been leaked onto peer-to-peer networks. Security pros can set up their own accounts on the most popular peer-to-peer networks, which include Gnutella, FastTrack, and eDonkey, and search to see if any information being offered resembles their proprietary data or intellectual property.

"Create a digital footprint for your company," Johnson says. Keep track of all searchable keywords that would lead a Web surfer to your company, including firm names, abbreviations, ticker symbols, brand names, subsidiaries, etc., and use those terms to search the peer-to-peer networks.

The idea for the Dartmouth study came from Homeland Security Department-sponsored work Johnson and his colleagues had been doing in studying international cyberattacks on U.S.-based targets. As the Internet increasingly becomes a part of the country's critical infrastructure, like telephone networks or power grids, Homeland Security wants businesses to protect themselves from cyberthreats.