

CNET News

February 15, 2006 10:29 AM PST

Beware the 'pod slurping' employee

By [Will Sturgeon](#)

Special to CNET News.com

Related Stories

[Consumers, retailers grapple with data theft](#)

June 22, 2005

[Survey: Congress falling down on data protection](#)

June 8, 2005

[Data for 600,000 Time Warner employees MIA](#)

May 2, 2005

[Bank of America loses a million customer records](#)

February 25, 2005

[ChoicePoint data theft widens to 145,000 people](#)

February 18, 2005

[Doctors prescribe iPods for storage](#)

February 7, 2005

[Ex-Austin student indicted for data theft](#)

November 5, 2004

[Disk storage outlook dimmer](#)

September 2, 2004

[Congressman raises offshore ID theft concerns](#)

February 25, 2004

A U.S. security expert who devised an application that can fill an iPod with business-critical data in a matter of minutes is urging companies to address the very real threat of data theft.

Abe Usher, a 10-year veteran of the security industry, created an [application that runs on an iPod](#) and can search corporate networks for files likely to contain business-critical data. At a rate of about 100MB every couple minutes, it can scan and download the files onto the portable storage units in a process dubbed "[pod slurping](#)."

To the naked eye, somebody doing this would look like any other employee listening to their iPod at their desk. Alternatively, the person stealing data need not even have access to a keyboard but can simply plug into a USB port on any active machine.

Usher denies that his creation is an irresponsible call to arms for malicious employees and would-be data thieves, and instead insists that his scare tactics are intended to stir companies into action to protect themselves against the threat.

"This is a growing area of concern, and there's not a lot of awareness about it," he said. "And yet in 2 minutes, it's possible to extract about 100MB of Word, Excel, PDF files--basically anything which might contain business data--and with a 60GB iPod, you could probably have every business document in a medium-size firm."

Andy Burton, CEO of device management firm [Centennial Software](#), said Usher walks a fine line but believes that he is acting with the best intentions and agrees that companies that still haven't recognized the threat need to be given a wake-up call.

"Nobody wakes up in the morning worrying about antivirus or their firewall because we all know we need those things, and we all have them in place," Burton said. "Now the greatest threat is very much inside the organization, but I'm not sure there are that many businesses (that) have realized it's possible to plug in an iPod and just walk away with the whole business in a matter of minutes."

Usher said companies shouldn't expect any help from their operating system, the most popular of which lacks the granularity to manage this threat effectively without impairing other functions.

"(Microsoft Windows) Vista looks like it's going to include some [capability for better managing USB devices](#), but with the time it's going to take to test it and roll it out, we're probably two years away from seeing a Microsoft operating system with the functionality built in," Usher said. "So companies have to ask themselves, 'Can we really wait two years?'"

Citing FBI figures that put the average cost of data theft at \$350,000, Usher argues that they can't.

"The cost of being proactive is less than the cost of reacting to an incident," Usher said.

Will Sturgeon of [Silicon.com](#) reported from London.

See more CNET content tagged:

[Burton](#), [threat](#), [Apple iPod](#), [minute](#), [Apple Computer](#)

