Encrypting Against Department of Homeland Security's New Laptop Search Policy

2008-09-24 16:04:58 by Southern

TORONTO

Computer security has never been more necessary. In the past, the threat of a security breach has come in the form of thieves: stolen laptops and PDAs, identity theft, and the like. These days the threat comes from a new ruling by a U.S. court. The Department of Homeland Security will now be allowed to confiscate laptops coming into the U.S. for an indefinite amount of time. Customs and Border Patrol will be able to search laptops or any other electronic device, download entire contents and keep the device for several days.

"This policy can create headaches -- or worse -- for unsuspecting travelers who don't plan ahead," says Jamie Brenzel, CEO of online data storage and backup service Data Deposit Box (www.datadepositbox.com).

Imagine your vital business accounting data being out of reach for days. Worse yet, what if your private financial information was exposed to the wrong people? What if a potential business partnership was leaked before the deal was made? Any of these scenarios is cause for concern. So what can be done?

Some experts suggest simply leaving electronics, such as laptops and PDAs, at home. While this strategy is easy enough for someone heading off on vacation, business travelers need more practical options to protect sensitive information. According to Brenzel, encryption is key to data protection. "Unfortunately, when it comes to data protection, many people would rather live by the idea that a security breach won't happen to them than try to figure out how to keep their data safe with encryption," says Brenzel.

Brenzel offers several tips to keep sensitive data safe. Travelers should:

-- Use the 'My Documents' folder and keep it on a separate disk partition. Partitioning a hard disk drive defines specific areas within the disk and makes it possible to create several file systems (either of the same type or different) on a single hard disk, increasing system efficiency. The partitioned drive will be difficult for someone to find, and the drive icon can be made invisible to make it even safer.

-- Store data on a remote server that can be accessed online. Files won't have to be downloaded onto laptops until they're safely across the border. Turning off the computer rather than simply putting it to sleep will also delete files that were visible on the remote server.

-- Password-protect drives and files, and fortify passwords by including different

characters, numbers, spaces, etc. NOTE: A border agent can require anyone to type in their password.

-- Delete old files that are no longer needed using a secure file erasure program, as well as Web sites, cookies and history.

In addition to encrypting laptops themselves, users should be certain their online backup provider not only backs up data, but also safely and automatically encrypts it off-site. Brenzel notes that the type of encryption used by an online backup provider is important. Users should compare speed, peer review and key strength when choosing a system. Popular encryption keys include Blowfish (used by Data Deposit Box), Triple DES and Khufu/Khafre.

MarketWatch
http://www.southernwolf.net//modules.php?name=News&file=article&sid=712