

BLOGS

Archives; Privacy & Information Security; Social Media & Technology; Workplace Policies

Lost in the Cloud: Dropbox, Data Insecurity, and Employee Shenanigans

For the uninitiated, Dropbox and other similar tools such as SkyDrive, Google Drive, or Cubby allow a user to log in to an account, upload documents or files to the cloud, and then access or download them from any device, anywhere at any time. Users can sync folders across devices and share or sync files with others.

Chances are, more than a few of your employees have discovered the ease and utility of cloud-based storage and file sharing tools. They are incredibly useful. But, along with the upsides that these tools offer like increased efficiency and team collaboration they also can cause serious data insecurity headaches for employers.

Here's a run-down of some of those risks:

1) Data Hackers:

While Dropbox disputes the allegation that it was hacked, usernames and passwords for over 7 million Dropbox users were compromised this past October. Employees using cloud storage to perform work tasks could leave company information vulnerable to the nefarious activities of others.

2) Employee Malfeasance:

Another data insecurity risk is employee malfeasance. There are a number of pending lawsuits alleging that employees used Dropbox or other cloud-based storage applications to misappropriate confidential company information. Unfortunately, sophisticated and savvy users of cloud-based tools sometimes help themselves to company information and documents and leave little trace behind. While a tell-tale sign of misappropriation is a flurry of email or downloading activity in the final days before an employee's departure, what if the employee regularly synced work files to a cloud-based application over a much longer period of time? Or, what if an employee routinely printed sensitive documents to a home computer? These are real risks to consider and try to prevent.

3) eDiscovery Nightmare:

Have you ever had to subpoena Google, or Facebook, or any other online provider to obtain data? It's not fun, easy, or quick. In addition, the process gives the person in control of the account at issue plenty of notice and time to cover up his or her tracks. And even if you do get your hands on some data, you may never be able to receive or recover the user access data that could reveal important details about when files were taken and what happened to them after that.

All of these potential scenarios leave an employer vulnerable to losing control of important records, potential trade secrets, and evidence to prove wrongdoing. In addition, to be able to establish a misappropriation claim against a wrongdoer, a company must demonstrate that it took sufficient, reasonable steps to protect its trade secrets and confidential information. If cloud storage and access is a free-for-all with no employer attention paid to what employees



are uploading, accessing or sharing with others, an employer may face credible arguments that it has not taken sufficient steps to protect its information.

So, take a good look at your technology use and social media policies. Do they address employee use of cloud-based storage? Do you have good systems in place to detect or block activity that could lead to a breach of information security? Is your company data vulnerable without you even realizing it? Depending on what you find, it may be time to roll up your sleeves and revise your employment policies and practices.