Elijah Yip, Esq.

Cades Schutte LLP
eyip@cades.com | (808) 521-9326 | www.legaltxts.com
Find me on: Twitter LinkedIn Google+

Cloudy With A Chance of Disaster: Avoiding the Security Risks of BYOC (Bring Your Own Cloud)

You've probably heard of BYOD (Bring Your Own Device). But do you know about BYOC? It stands for Bring Your Own Cloud, and it's more prevalent than you might think.

Cloud storage services like DropBox, Google Drive, and SkyDrive sport features that are attractive to an increasingly mobile workforce. They provide gigabytes of storage for free. Files in the cloud are accessible anywhere with an internet connection. Changes to a file in a cloud account are synced across all devices with access to the account. It's not difficult to see why cloud services are gaining popularity among individuals and companies alike.

Therein lies the problem. Because personal cloud accounts are so handy and easy to set up, an employee can create a security risk for a company in a matter of minutes. An employee can essentially connect the organization to the cloud without the company's knowledge via a private cloud account. This enables the transfer of confidential company data to a location outside the company's reach.

ComRent International, LLC v. Palatini, 2013 WL 5761319 (E.D. Pa. Oct. 24, 2013), involved such a scenario. ComRent hired Clayton Taylor to serve as a vice president of product development. Taylor primarily worked on matters related to Experium, a company that he co-founded and of which he was a minority owner. Taylor set up a Google Drive account to store, access, and edit all of Experium's intellectual property and confidential commercial information. Only Taylor knew the username and password necessary for the account. When ComRent hired an engineering firm to consult on options for the future of Experium, Taylor refused to grant the firm access to any of Experium's intellectual property, believing that ComRent might appropriate the intellectual property for itself. As a result, ComRent terminated Taylor and filed a lawsuit seeking access to the Google Drive account containing Experium's corporate files.

Here are some tips for avoiding problems with unauthorized use of personal cloud storage accounts by employees.

Set a Policy: Remaining silent—and therefore ambiguous—about the organization's stance on cloud storage can lead employees to believe they may use personal cloud accounts for work purposes without letting management know. To eliminate such misconceptions, set a policy on whether or not the organization will use cloud storage. If the decision is yes, then adopt measures to ensure responsible use of cloud storage. If the decision is no, then clearly

communicate to employees that storing work data in a personal cloud account is against company policy.

Maintain Control: If an organization decides to use cloud storage, it should retain control over the information necessary to access the cloud storage account (e.g., login credentials). It is advisable to create an account under the organization's name for official work purposes instead of allowing employees to use their personal accounts.

Restrict Unauthorized Cloud Services: Consider restricting access to private cloud storage sites from any device that can also access company data, including mobile devices, through the use of blacklists, proxies, and other network security measures. This will prevent the transfer of work files to a private cloud account. Organizations with BYOD programs might find it challenging to eliminate all access to private cloud services, but it is worthwhile consulting with the IT department about the feasibility of implementing such restrictions.

Retain Ownership: Make it clear that company information remains property of the company regardless of where it is stored. It's also a good idea to have employees sign written non-disclosure agreements.

Stay safe in the cloud!

Elijah Yip is a litigation partner at Cades Schutte LLP, a full-service law firm based in Honolulu. He is the founder and chair of the firm's Digital Media & Internet Law practice group. Elijah's practice is focused on commercial litigation, media law, and computer law.