7 Risks of Dropbox to Your Corporate Data

Introduction

We live in a world where information equals power. With the influx of online file-sharing solutions, distributing information has become easier than ever. As a result, it is now easier for information to fall into the wrong hands intentionally or unintentionally.

- Enterprise file sync-and-share, Terri McClure, Kristine Kao, TechTarget

Bring-your-own-device (BYOD) policies and an increasingly mobile workforce are putting new pressures on IT and changing the requirements for how workers want (and need) to access corporate data.

With over 200 million users, Dropbox has become the predominant leader for mobile file access. Unfortunately, what works for family pictures does not work with corporate files. In most cases, Dropbox quick to install, easy-to-use, consumer services present unacceptable security, legal and business risk in a business environment.

Here are 7 Risks of Dropbox to Your Corporate Data*

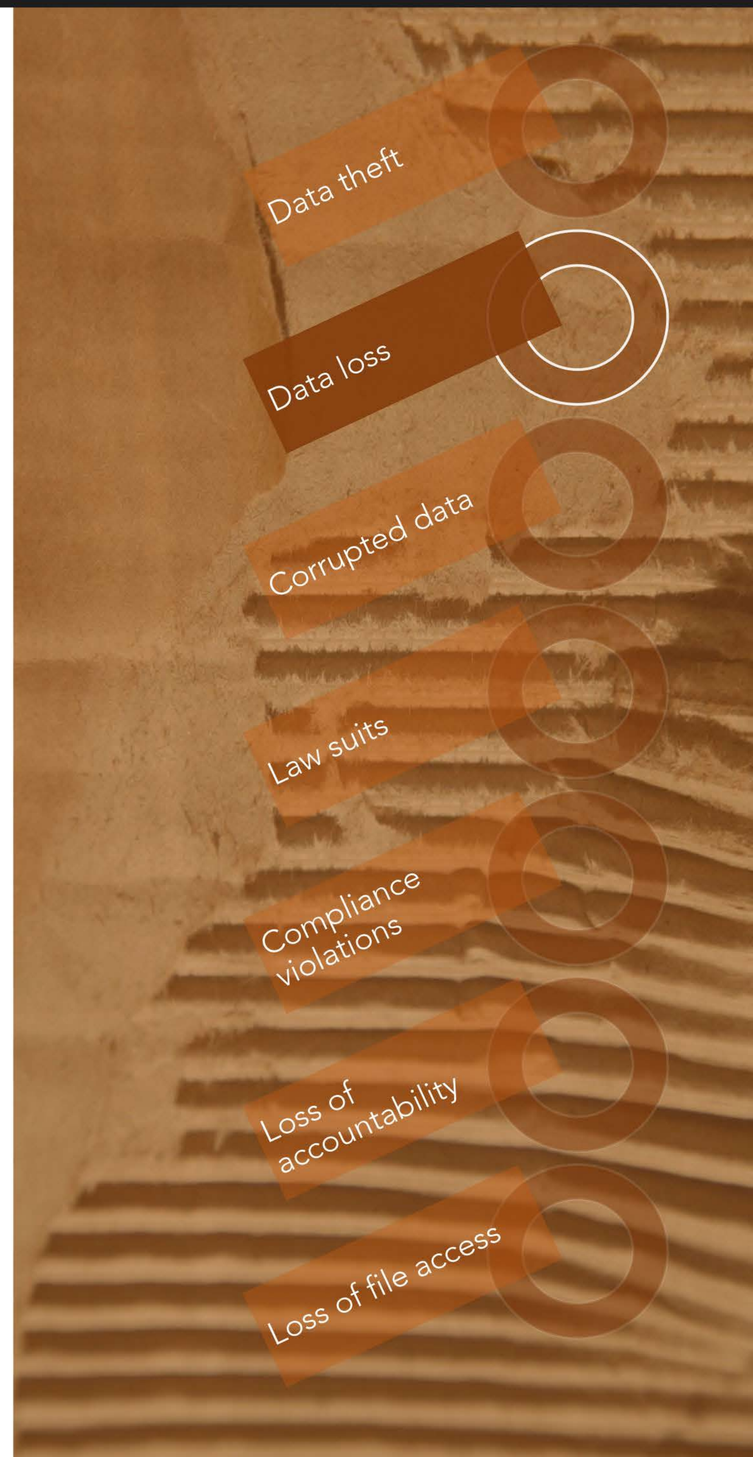
*All marketing claims refer to Dropbox Basic version 2.6.30 as of April 18, 2014

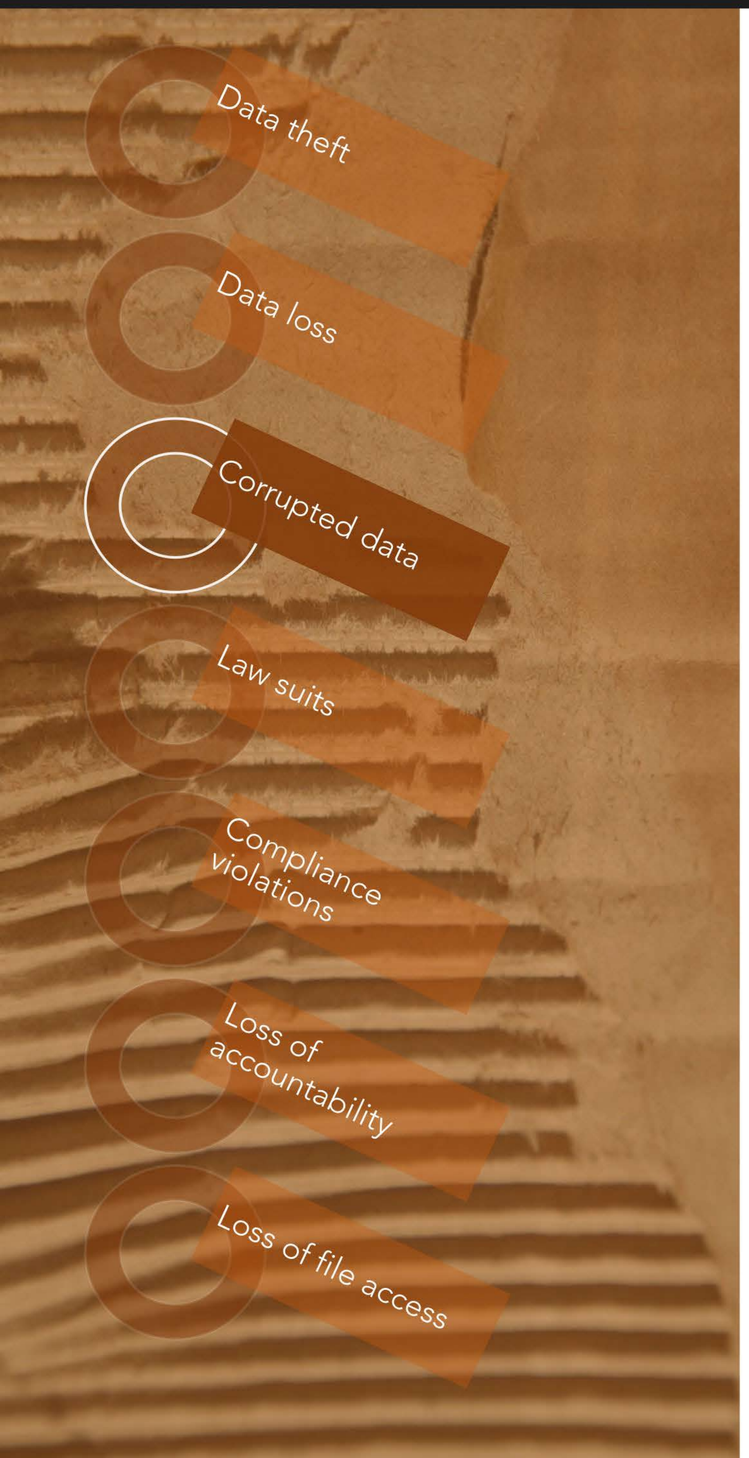
01
Data theft

Most of the problems with Dropbox emanate from a lack of oversight. Business owners are not privy to when an instance of Dropbox is installed, and are unable to control which employee devices can or cannot sync with a corporate PC. Use of Dropbox can open the door to company data being synced (without approval) across personal devices. These personal devices, which accompany employees on public transit, at coffee shops, and with friends, exponentially increase the chance of data being stolen or shared with the wrong parties.

02
Data loss

Lacking visibility over the movement of files or file versions across end-points, Dropbox can improperly backup (or not backup at all) files that were modified on an employee device. If an end-point is compromised or lost, this lack of visibility can result in the inability to restore the most current version of a file or any version for that matter.



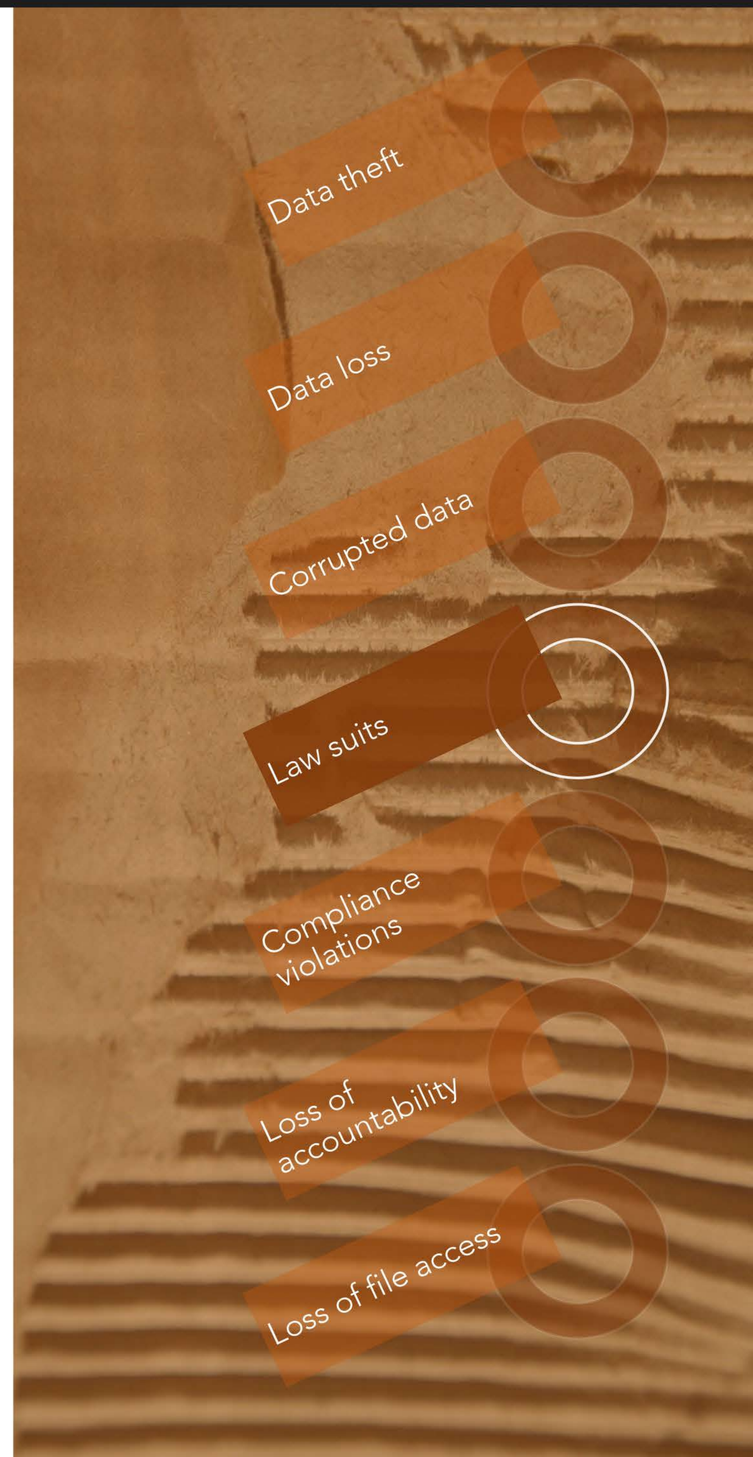


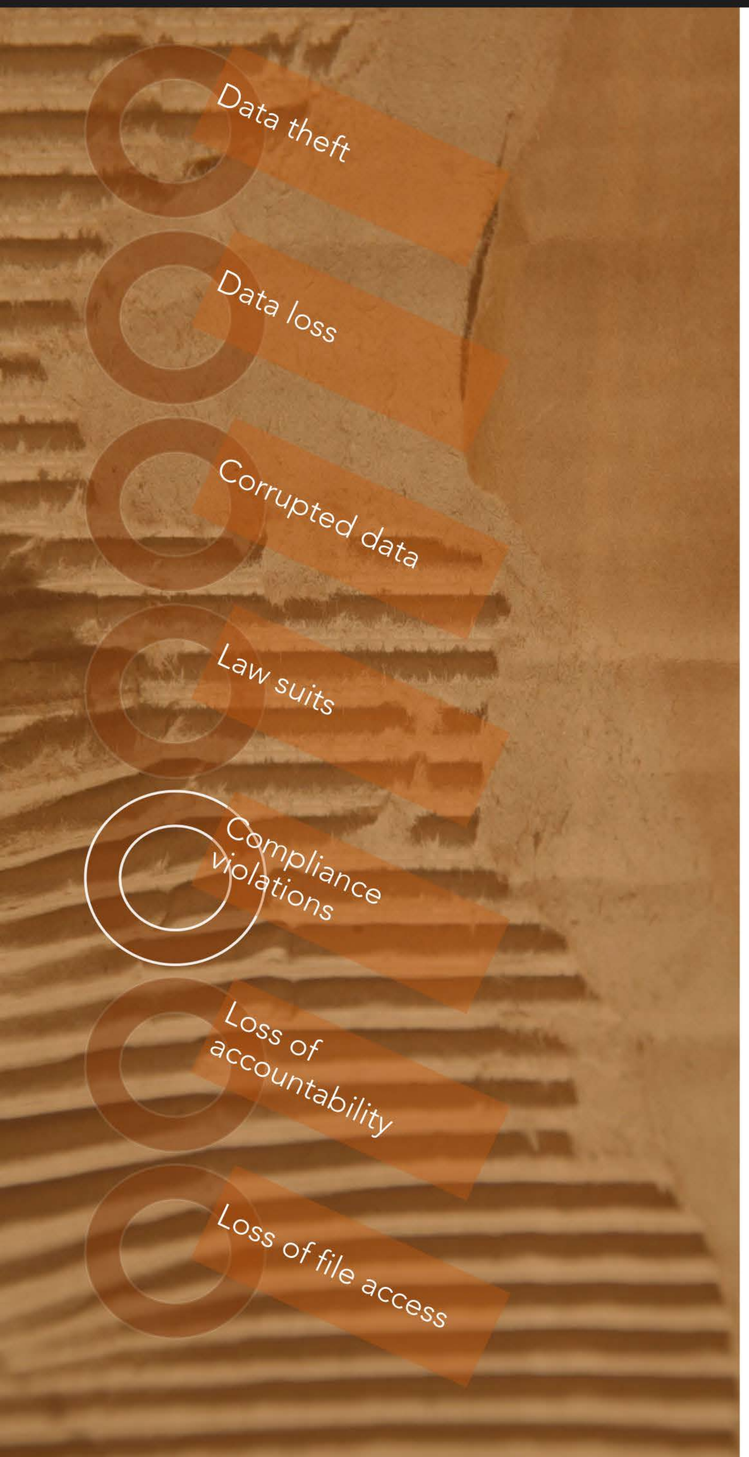
03
Corrupted data

In a study by CERN, the European Organization of Nuclear Research, silent data corruption was observed in 1 out of every 1500 files. While many businesses trust their cloud solution providers to make sure that stored data maintains its integrity year after year, most consumer file sync services do not implement data integrity assurance systems to guarantee end-to-end data integrity of the data, guarding against silent data corruption that has been shown to be common in large-scale storage systems.

04
Law suits

Dropbox gives carte blanche power to employees over the ability to permanently delete and share files. This can result in the permanent loss of critical business documents as well as the sharing of confidential information that can break privacy agreements in place with clients and third-parties.



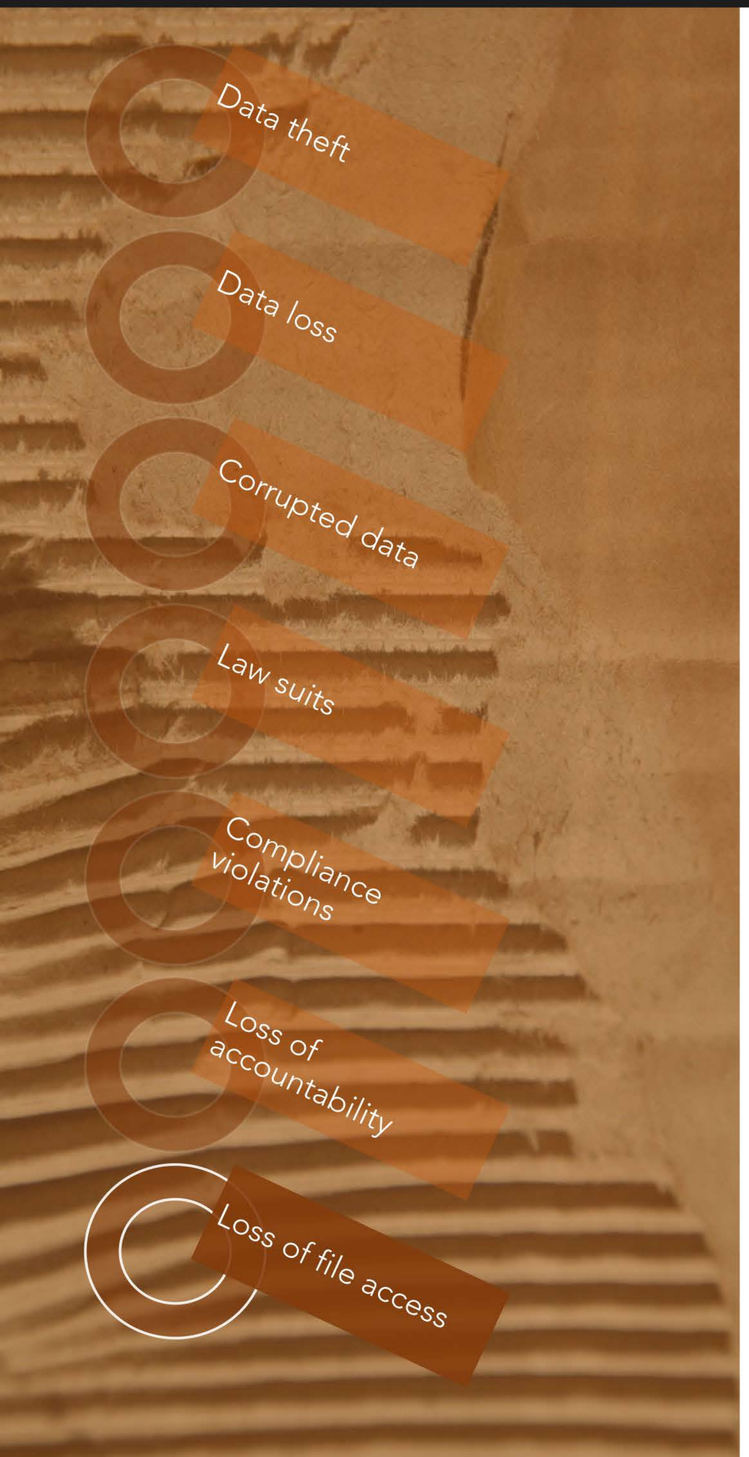


05
Compliance violations

Many compliance policies require that files be held for a specific duration and only be accessed by certain people; in these cases, it is imperative to employ strict control over how long files are kept and who can access them. Since Dropbox has loose (or non-existent) file retention and file access controls, businesses that use Dropbox are risking a compliance violation.

06
Loss of accountability

Without detailed reports and alerts over system-level activity, Dropbox can result in a loss of accountability over changes to user accounts, organizations, passwords, and other entities. If a malicious admin gains access to the system, hundreds of hours of configuration time can be undone if no alerting system is in place to notify other admins of these changes.



07
Loss of file access

Dropbox does not track which users and machines touched a file and at which times. This can be a big problems if you are trying to determine the events leading up to a file creation, modification, or deletion.

Conclusion

Dropbox poses many challenges to businesses that care about control and visibility over company data. Allowing employees to utilize Dropbox can lead to massive data leaks and security breaches.

Many companies have formal policies or discourage employees from using their own accounts. But while blacklisting Dropbox may curtail the security risks in the short term, employees will ultimately find ways to get around company firewalls.

The best way for business to handle this is to deploy a company-approved application that will allow IT to control the data, yet grants employees the access and functionality they feel they need to be productive.

If you would like more information on Anchor Cloud File Sync, please contact us at:

Office / Tech Center:
1408 N Sam Houston Pkwy East
Suite 130
Houston, TX 77032

Mailing Address:
9659 North Sam Houston Pkwy East
Suite 150, #233
Humble, TX 77396

IT service: (713) 489-4664
Tel.: (281) 901-0091
Fax: (888) 214-2980