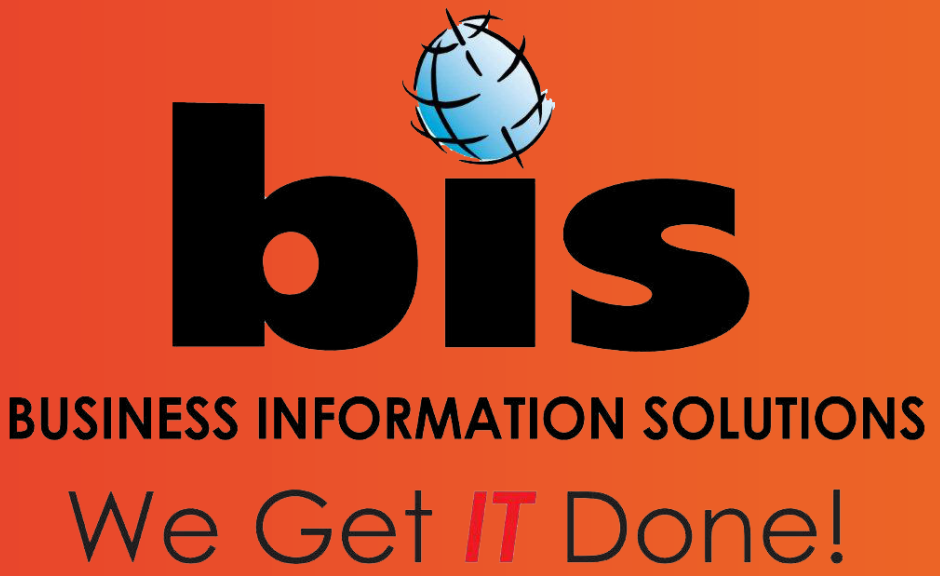
7 Risks Dropbox Poses to Your Corporate Data



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 400 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’s quick to install, consumer-grade services present unacceptable security, legal and business risk in a business environment.

Here are the 7 Risks Dropbox Poses to Your Corporate Data.

*All marketing claims refer to Dropbox Basic version 3.12.6 as of December 21, 2015

- Data theft
- Data loss
- Corrupted data
- Lawsuits
- Compliance violations
- Loss of accountability
- Loss of file access

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. The proliferation of these personal devices, which accompany employees on public transit, at coffee shops, and with friends, exponentially increases the chance of data being stolen or shared with the wrong parties.

02
Data loss

When administrators cannot manage and monitor file sync activities across an organization, they risk losing critical data. If an employee (or a group of employees) adopts Dropbox and starts using it to sync and share sensitive files, administrators without proper oversight cannot manage data sprawl, initiate remote wipes in the case of lost devices, and are unable to guarantee that files are properly shared with the right people.

- Data theft
- Data loss
- Corrupted data
- Lawsuits
- Compliance violations
- Loss of accountability
- Loss of file access

Data theft

Data loss

Corrupted data

Lawsuits

Compliance violations

Loss of accountability

Loss of file access

03
Corrupted data

In a study by CERN, the European Organization of Nuclear Research, silent data corruption was observed in 1 out of every 1,500 files. Dropbox and other consumer-grade file sync services disclose few, if any, details about how they prevent data corruption from occurring. True business-grade file sync services cryptographically tag every piece of data and redundantly store data on multiple data center racks to virtually eliminate any chances of silent data corruption, which has been shown to be common in large-scale storage systems.

04
Lawsuits

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, which can break privacy agreements in place with clients and third parties.

- Data theft
- Data loss
- Corrupted data
- Lawsuits
- Compliance violations
- Loss of accountability
- Loss of file access

Data theft

Data loss

Corrupted data

Lawsuits

Compliance violations

Loss of accountability

Loss of file access

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

Managers whose employees use Dropbox do not have access to detailed reports and alerts over system-level activity. As a result, administrators don’t have control of or visibility into how files have been edited, shared, or deleted. Business-grade, admin-controlled file sync services allow managers to view a comprehensive audit trail that details who touched or modified a file at any given point.

- Data theft
- Data loss
- Corrupted data
- Lawsuits
- Compliance violations
- **Loss of accountability**
- Loss of file access

Data theft

Data loss

Corrupted data

Lawsuits

Compliance violations

Loss of accountability

Loss of file access

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 problem if you are trying to determine the events leading up to a file creation, modification, or deletion. Moreover, at a moment's notice, files and folders may not be in their proper locations or readily available to employees.

Conclusion

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

While blacklisting Dropbox in the workplace may curtail the security risks in the short term, employees may ultimately discover loopholes, such as circumventing company firewalls or adopting another consumer-grade file sync service.

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 need to be productive wherever they are. Employees whose companies provide them with a secure, easy-to-use file sync service will see no need to bring Dropbox into the workplace.

If you would like more information on
BIS Cloud Sync, please contact us at:
Phone: 251-410-7601
Email: sales@askbis.com

BUSINESS INFORMATION SOLUTIONS

We Get *IT* Done!