Little-Known Facts about Dropbox

May 2015

Introduction

"As the BYOD trend continues, more and more businesses are faced with the growing reality of having their workforce go mobile and the potential associated security threats it poses for enterprises."
- Melissa Lewelling, CRN, June 24, 2013

With over 300 million users, Dropbox is the market leader in cloud file sync applications. Unfortunately, what works for family photos is not appropriate for corporate files. Dropbox is risky business. Beyond the risks of data loss, data theft, data loss, corrupted data, lawsuits, compliance violations, loss of accountability, and loss of file access, there are inherent flaws in the service that make it unsuitable for a workplace environment.

Here are some little-known facts about Dropbox — six things to consider before adopting Dropbox in the workplace.

1. Dropbox is the No. 1 most commonly blacklisted app

In general, BYOD and the advent of mobile applications has made employees more productive. But when it comes to mobility, there are some applications that companies should avoid. In a survey by Fiberlink of over 4,500 corporate and employee devices, Dropbox was the No. 1 most blacklisted app on iOS and Android. Business owners and IT administrators are blacklisting Dropbox applications because the popular file sync service lacks the administrative control and oversight necessary to avoid data leakage risks. Rounding up the top five blacklisted apps were SugarSync, Box, Facebook, and Google Drive. [i]

2. Dropbox shares can be accessed by anyone

Sharing with Dropbox is easy. Protecting your files with Dropbox? Not so easy. When a user shares a file or folder, Dropbox generates a public URL that can be accessed by anyone, without any password enforcement. In a study conducted by Intralinks, these fully clickable URLs were used to access sensitive files, including tax returns, a mortgage application, bank information, and personal photos. Intralinks also found evidence of intermingling of personal and corporate files. All of this begs the question: when you share files and folders with Dropbox, who are you actually sharing it with? [ii] [iii]

3. Dropbox only retains deleted files and revisions for 30 days

Business-class file sync services maintain a rich file and folder history so that companies may recall historical data, including deleted files and revisions. Moreover, retention of data is important for business that handle sensitive data and legally required for certain verticals. The Sarbanes-Oxley Act, the Federal Rules of Civil Procedures, tax laws, and other federal and local statues have distinct requirements for the retention of data. Dropbox's decision to permanently remove deleted files and revisions after 30 days is inconvenient and puts businesses at risk of legal and compliant disputes. If Dropbox customers want to retain deleted files and revisions for more than 30 days, they are directed to download and pay for a third-party application. [iv] [v]

4. Dropbox uses a single encryption key

Encryption is the primary safeguard against hacking and security breaches. Unfortunately for Dropbox customers, the keys to encrypt and decrypt files are with Dropbox - not on each user's machines. Worse yet, Dropbox uses a single encryption key for all customer's data. This insecure architectural design prompted Christopher Sighoian, a prominent security researcher, to issue an FTC complaint against Dropbox in 2011. His complaint alleged that Dropbox puts users at risk of government searches, rogue Dropbox employees, and even companies trying to bring mass copyright-infringement suits. In light of these charges, Dropbox scrambled to change language that appeared on its website. But the facts remain: Dropbox does not provide a way for users to encrypt files before they are transmitted to the cloud, Dropbox employees have access and can see the contents of a user's storage, and Dropbox has exposed its users to unnecessary risk of data theft by hackers, who if given the chance to break into the company's servers, may be able to steal users' data and the keys necessary for decryption. [vi] [vii]

5. Dropbox reviews your data to save costs

When a user uploads a file, Dropbox will review the data to see if it has been uploaded by a different user. If it has been uploaded before, Dropbox deduplication technology will point to the previously uploaded file, thus saving Dropbox from keeping two copies of the same file. According to Dark Reading (InformationWeek), "For starters, deduplication can make it easy for outsides to know what's already on the Dropbox servers, since the website studies a

file to see if it's seen it before." In sum, the deduplication technology imposed by Dropbox saves the company storage costs, but places your files at risk. [viii]

6. Dropbox does not guarantee uptime or offer live support

FAQs and Forums not good enough? Because Dropbox does not offer live support, you'll have to fill out a form for someone to get back to you. In addition, Dropbox has experienced outages, downtime, and security breaches over the years, causing business users to reconsider the reliability of the service. According to ReadWrite, "(Dropbox) checkered history of security breaches may make it a tough sell in the enterprise," including "a (2011) bug in the company's authentication mechanism, allowing third parties to log into user accounts and access files," and a 2012 breach that "allowed attackers to penetrate accounts used by Dropbox employees, including a document from which they may have been able to harvest email addresses...those email addresses were apparently used to send Dropbox users spam." In March of this year, Dropbox suffered an outage which caused errors and rendered the desktop and mobile file sync feature useless. In light of these events, a lack of live support is only the beginning of service issues that Dropbox faces. [ix] [x] [xi] [xii]

Conclusion

As your trusted IT service provider, we promise to work with you to minimize these risks and support your file sync needs. eFolder Anchor is a business-ready cloud file sync service that we stand behind and guarantee.

- Access files from anywhere
- Collaborate with ease
- Share files securely
- Control your data
- Eliminate FTP and VPN

Call us to learn how file access can be easy, safe, and secure.

Phone: 0845 644 0771
Email: sales@stratiis.com

[i] TechRepublic, Will Kelly, "Top mobile security concerns: Blacklisted apps and password protection," December 11, 2013
[ii] ReadWrite, Anthony Myers, "How Documents Stored On Box And Dropbox Could End Up On Google," May 7, 2014
[iii] CollaboristaBlog, John Landy, "Your Sensitive Information Could Be at Risk: File Sync and Share Security Issue, May 6, 2014
[iv] Dropbox Help, "What happens to my old and deleted file versions?" accessed on May 12, 2014
[v] ASAE, The Center for Association Leadership, "Designing a Compliant Electronic Record-Retention Policy for Your Association, July 2007
[vi] Gizmodo, Adrian Covert, "Dropbox Told Us Our Files Were Encrypted and Private. Turns Out They Aren't?," May 13, 2011
[vii] WIRED, Ryan Singel, "Dropbox Lies to Users About Data Security, Complaint to FTC Alleges," May 13, 2011
[viii] InformationWeek Dark Reading, Mathew J. Schwartz, "Dropbox Accused of Misleading Customers on Security," April 16, 2011
[ix] ReadWrite, Mark Hachman, "Dropbox To Business: Never Mind The Breaches, Come Store Your Stuff With Us!," April 10, 2013
[x] ZDNet, Zack Whittaker, "Dropbox hit by outage; file sync busted," March 14, 2014
[xi] ZDNet, Ed Bott, "Dropbox gets hacked … again," August 1, 2012
[xii] Dropbox Tech Blog, Akhil Gupta, "Outage post-mortem," January 12, 2014