Cloud Data Storage Solutions

Cloud Data Storage Solutions: Dropbox Security & Privacy Considerations

Dropbox is a cloud data storage solution that Higher Education security professionals are frequently asked to evaluate for the storage and sharing of institutional data. The issues of concern are common to most cloud data storage services; however vendor solutions and implementations vary greatly. The following outlines an evaluation of one vendor that can easily be applied to others, such as SpiderOak, box.net, Skydrive, and CrashPlan.

About Dropbox

From Dropbox: *"Dropbox is a service that lets you bring all your photos, docs, and videos anywhere, and share them easily. Any file you save to your Dropbox will automatically save to all your computers, your phone, your iPad, and the Dropbox website."*

Dropbox Features:

- 2 GB of Dropbox cloud storage space for free, with subscriptions up to 100 GB ($19.99 per month) available. 500 Mb additional increments available for each student referral.
- Work offline. Your files are available, whether you have a connection or not. Files are also available from the Dropbox website, wherever you login.
- Multi-platform. Dropbox works with Windows, Mac, Linux, iPhone, iPad, Android, and Blackberry.
- Dropbox stores your files using AES-256 bit encryption in the Amazon S3 service. Files are transferred from your device(s) to Dropbox using 256 bit SSL encryption (for supported devices).
- To save time and bandwidth, Dropbox only transfers the parts of a file that change.
- Share files with others by placing them in the (globally) public folder and sharing the URL, or share individual files and folders with specific Dropbox users.
- Restore all your files from the Dropbox website (e.g. after a disaster).

#Top of page

Considerations for Sharing Data

1. Data Leakage possibilities are magnified. Universities often secure individual servers, desktops, and even laptops with tools and controls. However synchronizing sensitive data from these local environments through Dropbox greatly increases the number of devices and networks which need to be secured for any particular file, potentially including multiple mobile devices and flash storage. Now there are many more copies of the data to be protected in much less defensible positions.
2. Data stored in public folders are available to the world. Dropbox works by having basically two types of folders, Public and Private. Private folders are restricted to the individual creating the folders, plus an access list of Dropbox users the creator may specify. Public folders on the other hand are available to anyone with the URL, can be searched (even by search engines such as Google if the URL is published) and should be considered as having no security whatsoever. It is easy to inadvertently publish files to the Dropbox public folder.
3. Location of the data in the Dropbox repository is not restricted to the USA. Dropbox uses the Amazon S3 service as their data repository. Amazon has several data centers world-wide; therefore US export restricted files should not be stored in Dropbox.
4. Dropbox is a convenient place to store and share personal files. Institutional data that is of a sensitive or proprietary nature, as well as valuable intellectual property, on the other hand, may not be appropriate for storage in Dropbox, because of the potential for unintended exposure.

#Top of page

Security Concerns and Issues

1. Information in the Dropbox servers is encrypted using AES, but with a common key for operational purposes, so that Dropbox administrators possessing the key can decrypt the user data in any folder. Dropbox asserts that this capability is used only by a very few administrators for support and debugging. However, any hacker uncovering the common key or a rogue employee could read any encrypted data. It is possible for the individual Dropbox user to encrypt files prior to placing them into Dropbox (e.g., using PGP or TrueCrypt), but this approach has not proved to be very elegant. In most cases, the entire file has to be re-encrypted, uploaded, and then synchronized with all devices each time it's changed, and there are no built-in key management capabilities.
2. Although most synchronization is accomplished using SSL to protect the data during transit and to identify the device being synchronized, certain mobile downloads are accomplished in the clear without SSL protection. Anyone obtaining the URL for one of these mobile endpoint synchronization targets would be able to intercept all of the synchronized data for both public and private folders.
3. Dropbox clients enable "LAN Sync" by default, adding a listening service to your local computer. Essentially, this is a peer to peer mechanism for syncing Dropbox files for a user with multiple Dropbox clients on the same local network, using cheap subnet bandwidth instead of 'expensive' internet bandwidth. LAN Sync runs a service on TCP port 17500 which listens for connections from anywhere in the world (unless specifically NAT'ed or firewalled) and broadcasts to the local broadcast domain on UDP 17500 looking for other Dropbox instances owned by the same user. Users accept the risk of allowing this communication to their client computers.
4. There have been significant problems with Dropbox's configuration files across computers. The impact of these is that someone else can steal access to your files by copying your configuration database file and effectively impersonating that computer's Dropbox credentials. It is rarely obvious that this has even occurred, end users of Dropbox would have to periodically login to the web application for Dropbox to see if the last

check-in from one of their computers originated at the right IP address. By copying the config.db file from a computer running DropBox an attacker can access and download all of your files without any obvious signs of compromise. Normal remediation steps after a compromise, such as password rotation, system re-image, etc., will not prevent continued access to the compromised Dropbox.
5. Dropbox offers third party developers an API for allowing their software to talk to Dropbox on behalf of a user and this access can include access to everything in the user's Dropbox. These permissions are not frequently audited by many end users and this technique provides another way for an unauthorized party to get access to data stored in a Dropbox.
6. Dropbox is examining content actively across users, ostensibly only for de-duplication. For example, if other Dropbox users have already uploaded the same file that you are uploading, Dropbox uses their copy without transmitting yours.
7. The vendor's change management procedures and communication to their users are of concern. A program update to the Dropbox service in June disabled authentication for the site's users for several hours. Essentially, anyone could access any account without a password. Dropbox estimated the exposure affected less than one percent of their accounts (which equates to about 250,000 users). On this basis they delayed announcement and then provided only limited public notification of the incident.
8. Dropbox does not require strong passwords, and does not integrate with locally provided (i.e., university directory-based) authentication services.
9. These are truly personal accounts. The institution would have no ability to retrieve information from an account, or transfer ownership, or close an account, if the user was no longer associated with the school. This has potential to enable continued access on the part of a terminated employee to institutional records stored with Dropbox.

#Top of page

Contractual Issues

1. Compliance with institutional contractual and regulatory requirements is difficult. More and more research and other contracts specify security provisions and restrictions on where and how the data may be stored. The Patriot act, FERPA, HIPAA, NIH, NSF, individual State Identity Theft Acts, and many other agencies and laws include provisions for the protection of the data and even the locations where it may be stored. It would be very difficult to get these security provisions validated for a distributed Dropbox synchronized folder implementation.
2. The terms of service for Dropbox are between the account owner and Dropbox. There is no opportunity to negotiate a "site license" agreement for your institution.
3. Dropbox does not have a mature enterprise licensing model. Instead of an enterprise site license, Dropbox has a business solution referred to as Dropbox for Teams (a pool of licenses that can be created for a group of user accounts). This solution allows a number of users to share storage quota, as it is bound to the team and not to individual accounts. They also offer something they refer to as Dropbox Rewind which allows for version control and rollback. This is included in the Dropbox for Teams model. Pricing for five or more "team members" starts at the annual price of $795 and includes 350 GB of shared storage. Additional users are $125 each and additional storage is $200 for 100 GB. At this time, there are no pricing tiers for higher volumes.
4. Files placed into your Dropbox account remain your personal property, but Dropbox may share information collected from you. The service provides one month of history (file level changes) in backup; any of which you can revert to and/or restore from. In addition, Dropbox states that they will not share your content with third parties for any purpose without being directed to do so by the account owner, however this does not apply to personal information that they collect about account holders.

#Top of page

Recommendations

- Use of cloud data storage solutions such as Dropbox should typically be avoided for storage of high risk institutional information. That is, a file that contains private or sensitive information, information that is covered by federal regulations, or that has a very high intellectual property value to your institution.
- On the other hand, information that is intended to be public may be safely shared using Dropbox.
- Always create a backup user account that has access to the Dropbox.
- Always ask your institution's information security officer or team to assist you to evaluate the appropriateness of using Dropbox for specific instances of institutional data storage and sharing.

#Top of page

Service References

- Box.net
- Crashplan
- Dropbox
- Skydrive
- SpiderOak

#Top of page

Questions or comments? Contact us.