The Dropbox Problem: It's Worse than You Think

Overview

The unsanctioned use of consumer-oriented file sharing services in business is a growing issue. It has been coined "the Dropbox problem" because of the prolific consumer file sync and share tool, but the difficulties apply equally to all consumer file-sharing services.

The migration of popular cloud storage services – most notably Dropbox – into the workplace is just one consequence of the rapid but inevitable consumerization of technology. These tools were designed to provide consumers with maximum convenience and ease-of-use, with little or no emphasis on privacy and security. These services have achieved massive popularity as a result of their simplicity, but at what cost to businesses unaware of the threats?

Some sync and share tools have begun to incorporate security, privacy and team collaboration as optional post-development add-ons, but the average user will not have access to these. End users will not typically take time to research and implement advanced configuration when quickly sharing files.

Beyond basic security issues, an important consideration is control and ownership; once information moves into an employee's personal cloud storage, a company has no control over who it is shared with or what else is done with it. Further, the organization does not have the ability to do any tracking or reporting, so there can be exposure to violating privacy laws unbeknownst to those tasked with assuring the company's compliance.

These serious problems can be broken down into four distinct areas. It's difficult to overemphasize the gravity of these issues, but here is a quick explanation of exactly what the problems are and why.

The failure to comply

The media has a litany of security criticisms of Dropbox and similar tools. These include hacking holes, authentication bugs and password breaches. These are worrying considerations for any individual, let alone a corporation. For businesses that are required to comply with privacy regulations, there is an even greater need to understand the breadth of compliance weaknesses in consumer sync and share tools. Weaknesses that are in breach

with data storage and transmission legislation such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the EU's 1995 Data Protection Directive.

For example, US HIPAA requirements state that only authorized users may access the protected data. While Dropbox touts that the data is encrypted, the encryption keys for the data are available to system administrators. This makes data susceptible to internal breaches, and violates HIPAA regulations.

Another administrative safeguard for compliance is password management. Under HIPAA, organizations must have: 'procedures for creating, changing, and safeguarding passwords. Users of personal sync and share tools have no regulations for creating complex passwords, or periodically changing passwords. The corporate IT department has no control over password policy, choice or use. Users could be protecting confidential, valuable data with a password that is simply "password" or the name of their pet. Further, because people frequently use the same password on multiple systems, discovery of passwords used on other systems can result in instant access to data on consumer sync and share services.

Finally, businesses need to have demonstrable tracking and reporting. Data movement shouldn't be invisible or unknown – as it is for any business with its data squirreled away by users on their personal sync and share services.

Business data needs to be protected for a number of reasons, not least regulatory compliance. But the potential damage caused by not protecting files isn't just going to affect the corporate lawyers – it will disrupt the lives of everyone working for that organization. Not only will the business be liable for huge fines, but also lost business and damaged reputations have a direct impact on the bottom line. The costs of such damage are difficult to calculate.

Who owns project files?

Collaborative working in team models is popular across modern businesses. As companies employ remote workers and outside contractors, the need for file sharing increases significantly. But business projects demand business tools. Sensitive project files must never be shared from a user's personal sync and share account. Once files are stored in personal accounts, they are essentially "owned" by the user of that personal account. This creates 2 problems: employees have copies of business files that they can make unauthorized use of, and projects may be hosted in an employee's account, and will be unavailable to other users when that employee leaves the firm.

In the first scenario, a sales person could leave the company with customer lists, copies of proposals and quotes, and internal sales strategy documents. This can be a serious issue if the employee goes to work for a competitor. An engineer could leave with product

design specifications. Again, this poses competitive risks. Or more simply, if any company confidential data is stored in a user's personal account, it is subject to all of the additional security risks discussed. And the problem of compliance extends to both current and former employees. If a company's data is exposed by a former employee, the company would still be liable for the compliance violation.

In the second case, a project folder may be created and hosted in a consumer sync and share service. All members of the team could be granted access to that folder and all relevant documents and images that it contains. This content is developed by a number of employees over a period of time, reflecting significant investment of time and human resources.

If a team is collaborating on a project that's hosted in a user's personal account, then the business could potentially lose all of the work and investment if the user leaves the company. The former employee has no responsibility to turn over content that is stored on his or her personal account. The repercussions of this type of project implementation could cost the business a great deal of money in wasted effort and redevelopment costs.

Because the business has no jurisdiction over a user's personal file storage accounts, there is nothing the business can do to recoup the lost files.

File sync is popular, but is it the best practice for business?

Syncing every file to corporate laptops is wasteful of resources; users can quickly run out of hard drive space by default. Is the company going to upgrade everyone's laptop to have an extra 100GB of storage? As a design feature, consumer services do this for speed and ease of use. For an individual laptop, owned by a consumer, storage may be less of a concern. But multiply this by hundreds or thousands of corporate laptops and it's an expensive approach. Not only is there a hardware cost involved, but the human resource requirements of your IT staff to perform needed upgrades can make this significantly more expensive than just hardware costs.

More troubling than the wasted resources of syncing every file is the serious security risk that this process presents. Synced files on lost or stolen laptops may be read with a simple disk scan utility. Changing the login credentials to the user's account would prevent access to the account, but would not limit reading the actual hard drive content.

In the United States, an estimated two million laptop computers are stolen, lost or misplaced in every year . The Ponemon Institute calculates that 12,000 laptops are stolen every week at airports and one in ten laptops will be stolen within the useful lifetime of the device .

Synchronization is a benefit for users in terms of improved performance and offline access to files. For example, if a user will not have internet access, and needs to continue to work

on a file, having an offline copy synced to the laptop is a productivity enhancement. Users need an easy way to sync only selected files that need to be accessed offline, and then have a mechanism for syncing and deleting the local copy upon reconnection. In commercial services, this can be difficult or impossible to do, and is the responsibility of the end user. It is critically important for business to be able to do this by policy, rather than by making users responsible for limiting synchronization of their data, and cleaning up the synced data when a local copy is no longer necessary. Synchronized data should also be encrypted in case the device is lost or stolen.

Security is not part of the architecture

Dropbox and other consumer services are attractive targets for hackers for a variety of reasons. Because these services are household names and are known to store extremely large caches of data, the chance of hackers getting valuable data is equally large. In addition, it is widely known that these services were developed for ease-of-use and large volumes of data storage. Security, corporate visibility into data usage, and regulatory compliance were not aspects of the design architecture. Leading providers of popular sync and share tools have been racing to retrofit security into the design- generally by being reactive each time a new security hole is exposed. But this begs the question: what holes have yet to be found?

The advent of software-as-a-service and the cloud enabled tech-savvy users to use consumer sync and share tools to circumvent security and to act as quick file-sharing workarounds. If this happens in the workplace and IT departments are too slow or otherwise occupied to respond, entire businesses could be at threat from malicious attacks or governing censure.

IT managers must be proactive and instead invest in Enterprise File Sync and Share (EFSS) services that are equally intuitive and acceptable to users as consumer tools, but provide visibility, compliance and security to the business. Security considerations should include:

1. IT policies for complex passwords
2. Encryption of stored data without the requirement of IT awareness of decrypt keys
3. On the fly encryption, so that unencrypted versions of files are not written to the disk in interim steps
4. Tracking and Reporting to assure appropriate usage, and to provide audit trails for access and sharing activities
5. Options for two-factor authentication

6. As-needed file sync capabilities with automatic deletion of re-synced files
7. Options for both on-premises and private cloud implementations
8. Ease of use for employees to facilitate rapid adoption of secure EFSS solutions
9. Implementation that easily integrates with existing data stores and authentication systems
10. Reverse proxy servers that do not write data, even temporarily, outside of the firewall in the DMZ

Conclusion

With myriad problems introduced by consumer-oriented sync and share tools, companies must find an alternative solution more fitting to enterprise needs. This solution must meet the ease-of-use expectations that these services have created while allowing IT departments to control and to monitor data and its usage, and also adhere to internal and external security regulations regarding the storing and sharing of data.

Fortunately, there are alternatives for organizations concerned by the public cloud, or which have privacy regulations that mandate on-premise solutions. An example that meets business criteria is Cornerstone MFT from South River Technologies. Cornerstone combines all the usability benefits of consumer file sync and share tools, with robust managed file transfer features, security and reporting.

Organizations need to think more seriously about the implications of employee file sharing, and how and where consumer sync and share technology may be present in their business. Employees need quick, easy file sharing in order to accomplish their work and keep business moving. But there is absolutely no time that you should trust a consumer-grade service with crucial business data. It simply presents too many risks. On-premise or private-cloud solutions with file encryption, reporting and IT control of the business data strike a great balance between employee productivity and adherence to IT security best practices.