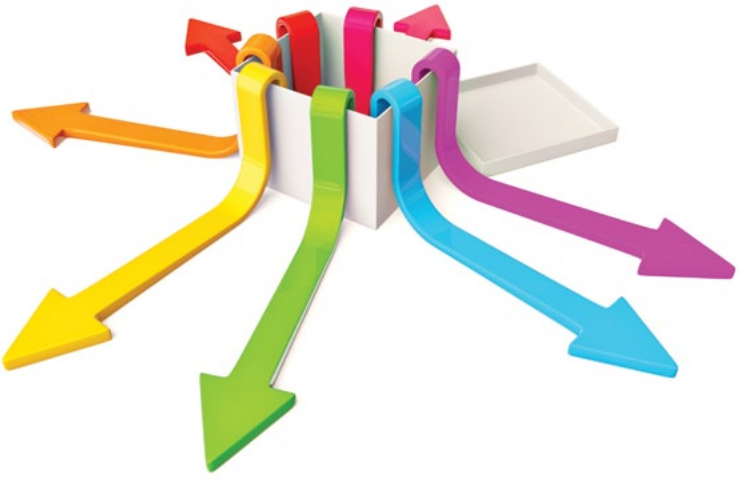
SOPHOS



Fixing Your Dropbox Problem

How the Right Data Protection Strategy Can Help

By **Chris Pace**, Senior Product Marketing Manager
and **Barbara Hudson**, Senior Product Manager

It's estimated that more than 50 million people have used public cloud storage services such as Dropbox to share and exchange files. Public cloud services are so easy to use that their openness can undermine existing IT policies regarding the transmission of confidential data. With data volumes threatening to overwhelm onsite storage, IT managers are looking to find a solution that's affordable and secure. This paper details a simple three-step approach to helping users manage access to the public cloud without placing your data or your business at risk.

Data is everywhere

What do we mean when we talk about cloud computing and "the cloud"? For the media, the cloud is the latest IT catch-phrase to describe next-generation offsite, virtual storage. For IT, it means a way to capture, contain, redistribute and manage zettabytes of data. For users, the cloud is a benign way to store information for themselves or share information with others who may be external to the company.

Cloud storage services like Dropbox—which boasts more than 25 million users as of April 2011—Egnyte or Microsoft's SkyDrive are useful tools that let people access their files from anywhere, on any device. But could that be putting your data at risk?

Today your users are working everywhere, so you need to make sure your data protection works everywhere too. This is especially true at a time when data breaches continue to bring unwanted media coverage to companies of all sizes and in all locations.

More than 4 million records were breached in 2010 alone, according to the Verizon 2011 Data Breach Investigations Report. And more than 92% of those breaches were the result of external hackers rather than an insider or business partner. Moreover, the cost of a data breach continues to rise. The Ponemon Institute's latest U.S. Cost of a Data Breach report shows that data loss cost organizations $214 per compromised record at an average of $7.2 million per data breach event.[1]

It's simply never been more important to secure laptops, disk drives, files on your servers, stored in the cloud, or accessed from mobile devices. Your users may already be using the public cloud without your knowledge or approval. When you think about security in the cloud, you should think about what that means for your business data.

- Are your users uploading files to the cloud?
- What services are users accessing and how?
- Do the files contain sensitive business data?
- Are these files unencrypted?
- Do you know where your data is archived?

1. Ponemon Institute, *Second Annual Cost of Cyber Crime Study: Benchmark Study of US Companies*, August 2011

The cloud is everywhere

Cloud storage providers have full access to your data and control where it is stored. You may know where a cloud managed service provider's (MSP) storage facility is located geographically. But generally you won't have specific information about the infrastructure or security mechanisms your MSP has in place. For example, is your data archived in a multi-tenant or isolated container? Does it use SAS-70 or environmental controls?

Cloud storage becomes even more problematic when you consider the need for data compliance. Your data might not even be stored in your home country. This could frustrate an auditor evaluating your data's level of security and chain of custody. There is also the risk that unauthorized users could access sensitive, regulated information because it wasn't properly secured due to a lack of controls, processes and procedures.

In a 2011 Ernst & Young survey, 61% of organizations were either already using or planning to evaluate cloud storage. However, more than half of organizations (52%) had yet to put controls in place to mitigate data risk.[2]

In less than a generation we have made the leap from storing data on a USB flash drive to cloud storage, from accessing our work documents over a VPN to using services like Dropbox. The consumerization of IT, and the availability of high-speed Internet connections at work, at home and everywhere through mobile devices, has changed how we access and store our data.

These changes give users power and autonomy. And in most cases users will choose the services they know and like, rather than strictly following corporate IT policies. But there is risk in giving users too much control.

4.0

Million records breached

in 2010 alone, according to Verizon 2011 Data Breach Investigations Report.

7.2

Million dollars per data breach event

Data loss cost organizations $214 per compromised record.

92

Percent of breaches were by external hackers

rather than an insider or business partner.

2. 2011 Ernst & Young Global Information Security Survey

Limitations of a digital "do-it-yourself" approach

In the absence of well-defined policies, education for end users, and officially supported alternatives for sharing files, knowledgeable end users will overlook security and compliance concerns in favor of easy alternatives. These alternatives include consumer-oriented "dropbox" solutions, non-commercial FTP servers, transferring files as email attachments, and custom in-house programs and scripts.

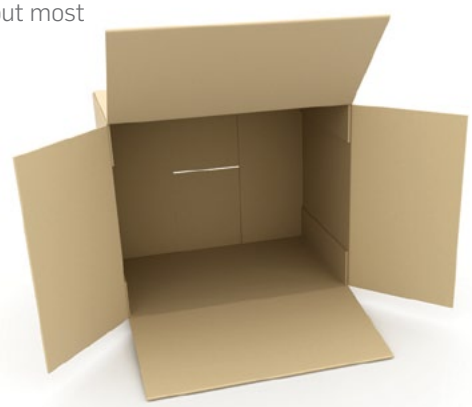
Because these solutions are widely available for free, for almost all computing platforms, they have found their way into organizations of every size and can often become embedded in critical workflow.

Limitations of consumer-oriented dropbox solutions and custom in-house programs

- **Unsupported infrastructure:** Consumer-oriented solutions likely do not support enterprise-grade requirements. Custom programs and scripts may have been developed by people who have long since left the company.
- **Unenforced policies:** Because these capabilities are based on consumer-oriented solutions or custom development at different points in time, they may not reflect the organization's current policies for security and compliance.
- **Unacknowledged risk:** Organizations that continue to share files using these non-supported environments may not make a conscious assessment and acceptance of the inherent risk. The traditional tension between enterprise policy and end-user productivity plays out most strongly in this area.

Limitations of transferring files as email attachments

- **File size of attachments:** Typical enterprise email configurations restrict attachment sizes to 10mb or less.
- **Performance:** Email was not designed to handle extremely large files. Timely and reliable delivery often proves problematic.
- **Storage:** Large attachments (often multiple copies of large attachments) quickly eat up allocated storage. Small attachments with widespread distribution can have the same effect.
- **Security and compliance:** Too often policy enforcement depends on individual end users doing the right thing, versus automated enforcement by solution providers.



Source: Aberdeen Group, January 2012

Develop a strategy to protect your data in the cloud

To decide what's best for your organization and your users, ask yourself the following questions:

- Who administers your data?
- Do you remain in control of your data?
- What are the consequences of a data breach?
- What is the probability of data loss?
- Can you account for your data's security?

You may not get the best answers to these questions if your users are accessing cloud services without your knowledge, consent or encryption policies applied. And if you're not yet controlling user access to cloud-based storage services and applications or encrypting all your sensitive files, it's time to start.

There are still three simple steps you can take to increase the responsible use of cloud services while maximizing data protection for your business.

1. Apply web-based policies using URL filtering

You can control access to websites like Dropbox.com with URL filtering, which prevents users from browsing to forbidden sites. You can also decide to permit access on a case-by-case basis with multiple profile settings, so that selected users retain access and others are denied it.

2. Apply application controls

Use application controls to set policies for the entire company or specific groups to block or allow particular applications. In the case of Dropbox.com, application controls prevent people from installing and running this application and block the Dropbox executable.

3. Apply data encryption

Automatically encrypt files before they are uploaded to the cloud from any managed endpoint. With password access to encrypted files, users can still access the file from anywhere or any device.

Control your data with an encryption solution

An end-to-end solution for directly managing the encryption of data stored locally or in the cloud allows users to define, manage and own their encryption keys to secure designated files. Users can have access to files at any time, whether behind the firewall or in the cloud, as well as consistent encryption standards at every point. For example, SafeGuard Encryption for Cloud Storage keeps all files encrypted, regardless of whether they are copied or moved to another drive, network or device.

An encryption solution allows users to choose their preferred cloud storage services because the files are always encrypted and the keys are always your own. And because encryption takes place on the client before any data is synchronized, you have full control of the safety of your data. You won't have to worry if the security of your cloud storage provider is breached.

Central keys give authorized users or groups access to files and keep these files encrypted for everyone else. Should your web key go missing for some reason—maybe the user simply forgot the password—the security officer inside the enterprise would have access to the keys in order to make sure the correct people have access to that file.

Additionally, you can also create Dropbox.com accounts for individual business units. For example, human resources (HR) can encrypt all their files in Dropbox with a password that all of HR knows. If someone in HR accesses those files from their enterprise laptop, they are already carrying the key, allowing them to view and share files with colleagues on demand and as appropriate.

With SafeGuard Encryption for Cloud Storage it doesn't matter where you access files for your cloud storage service—your home computer, corporate laptop and, starting in 2012, file readers for iOS (e.g., iPhone, iPad) and Android devices. Note: Encrypted content can be viewed but not modified on these devices.

Data risk case study: employee theft

Here's a scenario where leaving files unencrypted could really harm your business. Your business has a banner year, but when word leaks that sales staff will not be receiving the discretionary year-end bonus, one of your key sales employees decides to pursue an opportunity with a competitor. She knows that her customer and prospect information will be of great help to her, but she's also aware that the company's IT department has security measures in place that will alert them to the downloading of files from her work station.

After spending just a few minutes on the web, she learns how to install a free app on her iPad that gives her remote access to her work files. With the help of her new app she secretly copies to her iPad all of the confidential records she has accumulated over the last few years. Next, she meets with the sales manager of your biggest competitor and with the information on her iPad entices her potential new employer. With offer letter in hand, she gives her notice and departs without your IT staff knowing that proprietary information has been taken from your secure network.[3]

3. Courtesy of Sheehan Phinney Bass + Green PA, www.sheehan.com.

Get comfortable in the cloud

Data is not a static asset of your business. It grows, it changes, and it influences the arc of your organization's success today and well into the future. In that way data requires security, protection and confidentiality. Data is also meant to be shared—with employees, partners, management, boards of directors and others who are invested in the performance of your business.

The increased use of smartphones and tablet PCs represents a major shift in the way people collaborate. If you provide your workers with such devices, or even allow them to use their own as part of your "bring your own device" (BYOD) policy, it opens up a wealth of opportunities for increased employee comfort and productivity.

But enhanced mobility can increase both productivity and flexibility only if the right tools are in place. The use of cloud storage is one such collaboration tool. Unless you provide a flexible alternative in your own enterprise cloud, blocking such services could hinder the success of your mobile strategy.

Still, take nothing for granted. As long as there is data ready to be accessed and shared there are external services available to help your users do just that. Mostly their intentions have upside such as increased productivity. Other times they find it easier to overlook what they believe to be overly-restrictive procedures that inhibit rather than foster best practices.

Users would argue that it's easier to use a Dropbox-like service than it would be using a VPN or simply emailing themselves the data. Or, more problematically, carrying it with them on an unencrypted and unprotected USB.

Determine how and where files shared among these individuals and groups can occur. You set the bar on whether information stored in the cloud is allowed, denied or permissible under certain circumstances and to whom those permissions apply.

Use case: Sharing files securely in the cloud

Imagine your business is a U.S. supplier for an international manufacturer. The computer-aided design drawings your team has rendered are too large to be transferred to your counterpart in Europe, and FTP servers on both sides of the Atlantic do not support encryption. They also lack the ability to send verification that a transfer is complete and verification of the integrity of the file. By using SafeGuard Enterprise 6 to encrypt the file before using Dropbox, your counterpart in Europe can browse to his Dropbox account, open it and easily retrieve the drawings and begin evaluating the product's cost to produce and manufacture.

SafeGuard Encryption for Cloud Storage

SafeGuard Encryption for Cloud Storage helps you to make peace with your end users and gain their trust to do the right thing. Instead of preventing end users from doing something they're used to, you can apply enterprise policies and solutions that will help them achieve their goals in a way consistent with the IT policies and corporate standards of your organization. This includes:

Protecting your data in the cloud. You stay in control of the encryption keys. And only people with those keys can access your valuable data.

Securely sharing your confidential data with your team members. You can even share with third parties without compromising on security.

Perform encryption transparently and in the background. Allow your users to work without interruption.

Deliver security with proven data encryption algorithms for the best protection and performance.

End-to-end data protection for data stored on hard drives, flash drives, file shares and in the cloud.

See how it works

Request a free trial of SafeGuard Encryption for Cloud Storage

United Kingdom and Worldwide Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia and New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

Sophos Whitepaper 3.12v1.dNA

SOPHOS