

Shadow IT in the Enterprise



Confessions from More
Than 1,000 Enterprise Users

Introduction

In today's work environment, the proliferation of smartphones and tablets is driving mobility and a corresponding culture of convenient, "always on" access to information. More than ever before, employees are demanding access to their files – at any time and from any device. Furthermore, this culture of access is contributing to more distributed environments, with teams in multiple offices needing to work together across the boundaries of physical locations.

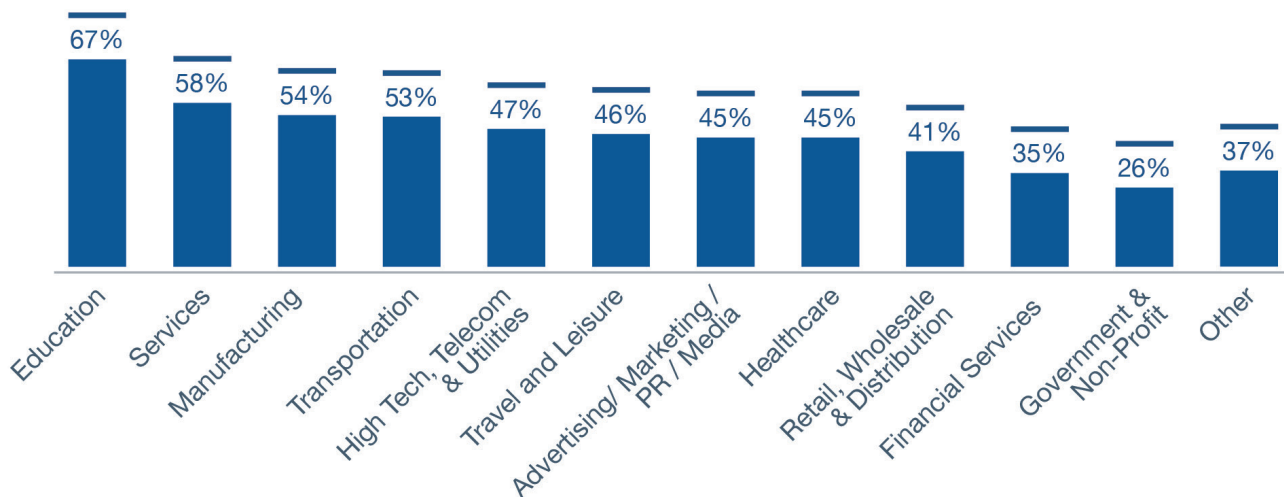
Oftentimes, the expectation for convenient access from anywhere is outpacing IT's ability to deliver. Consequently, users are turning to file-sharing solutions geared toward consumers, such as Dropbox, to fill this gap. This concept of using software solutions without IT approval is referred to as "Shadow IT". Solutions in Shadow IT are unmanaged, unmonitored and unsupported by IT, putting the data stored in these solutions at risk of loss and exposure to unauthorized users.

Companies aware of the risks associated with Shadow IT work to eliminate, or at least mitigate, this risk by implementing policies prohibiting the use of unapproved solutions. However, policies alone are not effective; organizations must consider providing solutions that are approved by IT and deliver the functionality that users demand.

In September 2012, Nasuni conducted a survey of more than 1,300 corporate IT users to better understand employee habits regarding Shadow IT and their impact on corporate IT systems and security. This paper presents the survey results, including what users revealed about their use of consumer file sharing solutions and personal devices.

Who Uses Dropbox at Work?

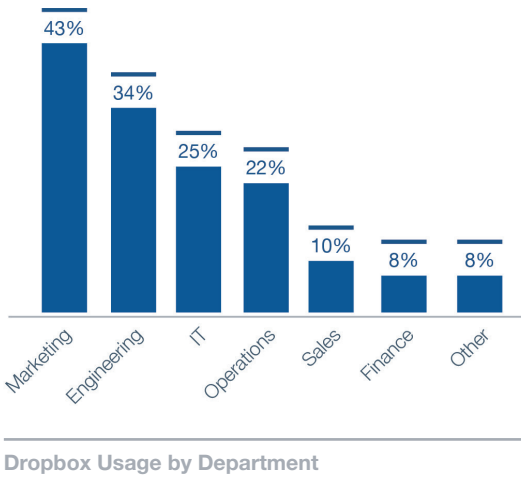
Dropbox is one of the most commonly employed file sharing services in Shadow IT, offering a simple tool for file storage and sharing. According to Dropbox, the number of registered users is growing exponentially and is currently at 100 million users worldwide¹.



Shadow IT (File Sharing) Usage by Industry

¹<http://www.forbes.com/sites/victoriabarret/2012/11/13/dropbox-hits-100-million-users-says-drew-houston>

It is commonly understood that people use Dropbox to share personal photos, videos and documents. The question is – how many people are using Dropbox for work? And, perhaps more importantly, do organizations have a clear view into who is using Dropbox?

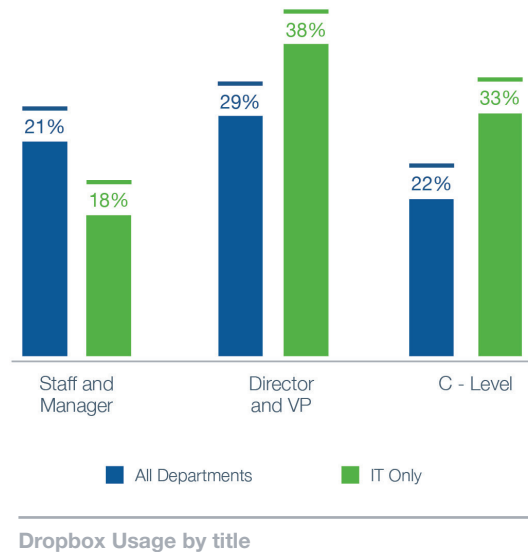


According to the survey, 1 out of every 5 respondents is placing work files at risk in a personal Dropbox account. In the process of leveraging file-sharing services users are storing files outside of the managed IT infrastructure in a solution that does not provide enterprise class security or control.

The frequent use of Dropbox at work, combined with the security concerns, is one of the most troubling aspects of Shadow IT. A critical step in addressing the risks is understanding who in the organization is leveraging this tool.

After an organization identifies who is leveraging Dropbox, the next step is to understand what type of files reside in it – are they public or private files? While it is possible that the files stored in Dropbox contain non-sensitive information, it is more likely that users have become accustomed to using these services for all files, including sensitive content.

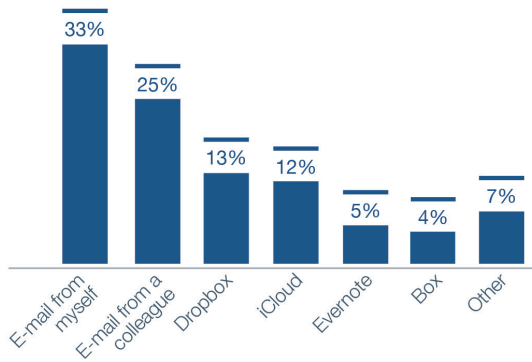
The sensitive data stored in Dropbox is not secure and just as importantly, not controlled by IT. This means that if an employee leaves the company, the information that user has stored goes with them, creating a significant risk of data loss or exposure. Furthermore, as the amount of sensitive corporate data stored in Dropbox increases, the online file-sharing service will become a more attractive target for hackers and other malicious groups.



The Move to Mobile

Beyond using file-sharing services on desktops and laptops, users are leveraging smart phones and tablets to access work files, attaining the speed and flexibility they need for high productivity in a mobile world.

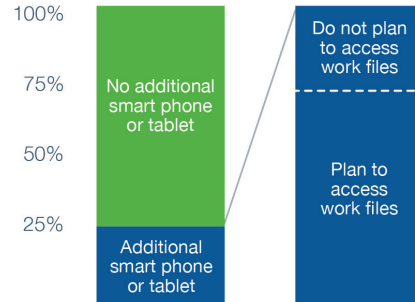
3 out of 5 users with a personal mobile device resort to using their own device to access work files because the company does not provide the tools they require. Dropbox usage is prevalent in the mobile world as well; after e-mail, it is the most common tool used for accessing work files on a mobile device.



Tools Used to Access Work Files on Personal Mobile Devices

As the number of devices grows, the use of Dropbox and Shadow IT will simultaneously increase to meet the demands of new users. 1 out of 4 survey respondents plan to have an additional smart phone or tablet before the end of the year. This rapid

growth of mobile devices will naturally drive demand for accessing work files; 73% of respondents who are planning to acquire a new device say they will use the device to access work files.



Increasing Mobile Devices in the Workplace

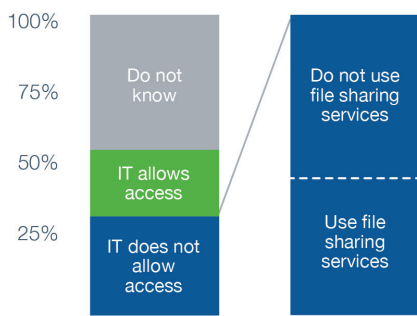
Policies for Protection

A critical part of implementing an effective IT policy is raising awareness of the policy among users. The survey data shows that almost half of all respondents do not know the company policy on accessing file-sharing services, indicating that these companies either do not have policies or have not effectively communicated the policy to the users. However, companies that have educated their users about corporate IT policies have not fully addressed the problem with Shadow IT either. Our survey suggests that 49% of users do not follow IT policies even when educated about the policy.

Are you wondering who your Dropbox users are? Survey data shows that a smart phone or tablet user is 3x more likely to use Dropbox.

What is the policy – access or no access? 54% of respondents work at organizations that do not allow access to file sharing services, while 46% work at organizations that do allow access to file sharing services.

An effective IT policy requires both education and participation. Without sufficient knowledge and user participation, IT will continue to face challenges with Shadow IT.



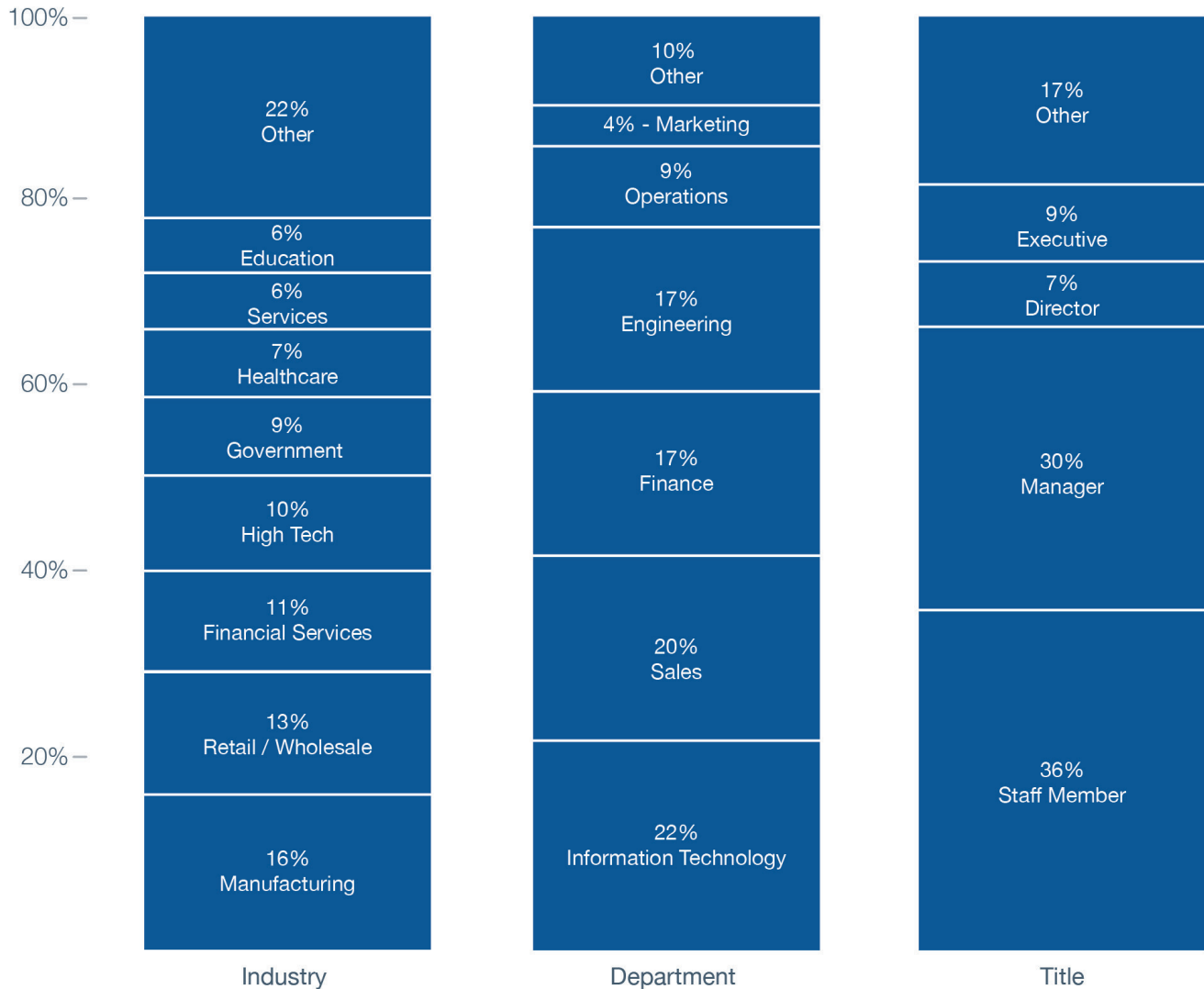
Company Policy for File Sharing Services and User Behavior

Conclusion

As smart phone and tablet usage grows in adoption, the growth of Shadow IT will likely continue, fueled by users' requirements for anytime, anywhere access to files. Furthermore, policy and education alone do not address the emergence of Shadow IT and resulting unmanaged file sharing and data exposure. In order to fully address this issue, organizations must consider providing the tools that deliver the convenient and flexible access to information that users want. Without the proper tools provided, managed, and supported by IT, users will continue to find alternative solutions and work around existing policies, leaving IT in the dark.

The Respondents

More than 1,300 corporate IT users responded to the survey from a range of industries, departments and levels in the organization. In some cases, data was analyzed to compare IT vs. non-IT users to better understand the unique behaviors of the different groups. The demographic breakdown of respondents is:



Survey Demographics

About Nasuni

Nasuni offers a powerful Storage Infrastructure as a Service: a uniform, complete storage solution delivered as a service, enabling distributed organizations to offload the management of the storage infrastructure (including backup, replication and offsite protection) and consume storage on-demand, without any change to the way users access information. With Nasuni, corporate data is uniformly available in all locations, enabling organizations to increase user productivity, streamline costs and improve business agility.

Our team is made up of enterprise storage, security and networking industry veterans with a shared vision of transforming the way enterprise organizations view data storage. We believe that storage should be as easy to purchase, consume and manage as the electricity that keeps the lights on.