WHITE PAPER

# Do Ex-Employees Still Have Access to Your Corporate Data?

**An Osterman Research White Paper**

*Published August 2014*


**Osterman Research, Inc.**
P.O. Box 1058 • Black Diamond, Washington • 98010-1058 • USA
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com
www.ostermanresearch.com • twitter.com/mosterman

# EXECUTIVE SUMMARY

Organizations of all sizes have a problem that most of them are not addressing adequately: their employees store corporate data on various file-sharing and content-access platforms and most of these people still have access to this data after they are no longer employees.

Worse, much of this data in what we are calling "rogue applications" is sensitive or confidential and many former employees continue to access it and – in some cases – share it with others.

The ramifications of this problem are quite serious for organizations of all sizes and in every industry:

- They can run afoul of data breach laws or other regulatory requirements by allowing non-employees and others to have access to sensitive or confidential information.
- They may not be able to implement legal holds or satisfy eDiscovery requirements if they do not have complete control over their data.
- They can lose intellectual property and even future rights to it.
- There are a variety of other problems that can result, such as ex-employees who now work for a competitor having access to confidential information, ex-employees deleting data that is still in use by his or her former colleagues, malicious ex-employees who willfully delete or modify information, and unrealized efficiencies and economies of scale if various teams across an organization are deploying redundant services independently.

In order to address these issues and mitigate the enormous and growing risk that they face, organizations need to:

- Understand the seriousness of the rogue applications problem and how it increases corporate risk on a variety of levels.
- Ensure that they know where their data is located and how it can be accessed quickly and efficiently.
- Formally ask departing employees for all of their login credentials and ensure that ex-employees agree to abide by rules for accessing data they used in their previous employment.
- Establish policies about the appropriate use of various apps and cloud-based tools.
- Provide good file sharing, cloud storage, Webmail and other alternatives that will enable employees to do their work and keep IT in control of corporate data.

## ABOUT THIS WHITE PAPER

Osterman Research conducted a survey to quantify the extent of the rogue applications problem. In order to qualify for the survey, respondents had to use a computer for work for more than 50% of a typical workday in their current job and in a previous job. A total of 379 online surveys were completed during June 2014.

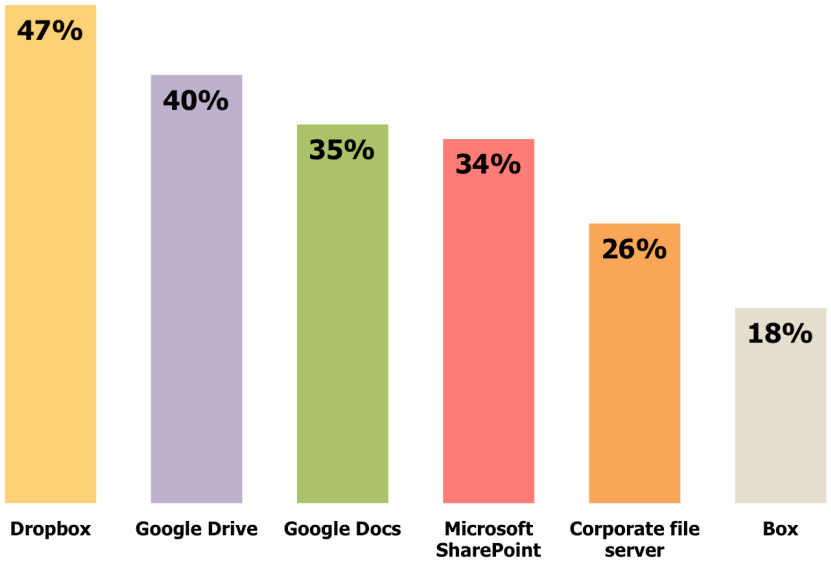
***Employees store corporate data on various file-sharing and content-access platforms and most of these people still have access to this data after they are no longer employees draft.***

# EX-EMPLOYEES HAVE ACCESS TO CORPORATE DATA FROM THEIR PREVIOUS EMPLOYERS

## MOST EMPLOYEES USE PERSONAL FILE-SHARING SERVICES

Our research found that 68% of information workers store work-related information in a personally managed file-sharing solution, such as Dropbox, Google Drive or Box, among many others. Moreover, as shown in Figure 1, Dropbox was the most commonly used file sharing or content-access platform employed in a previous job, followed by Google Drive, Google Docs and Microsoft SharePoint.

**Figure 1**
**Leading File-Sharing and Content-Access Platforms That Were Used in a Previous Job**




*Source: Osterman Research, Inc.*

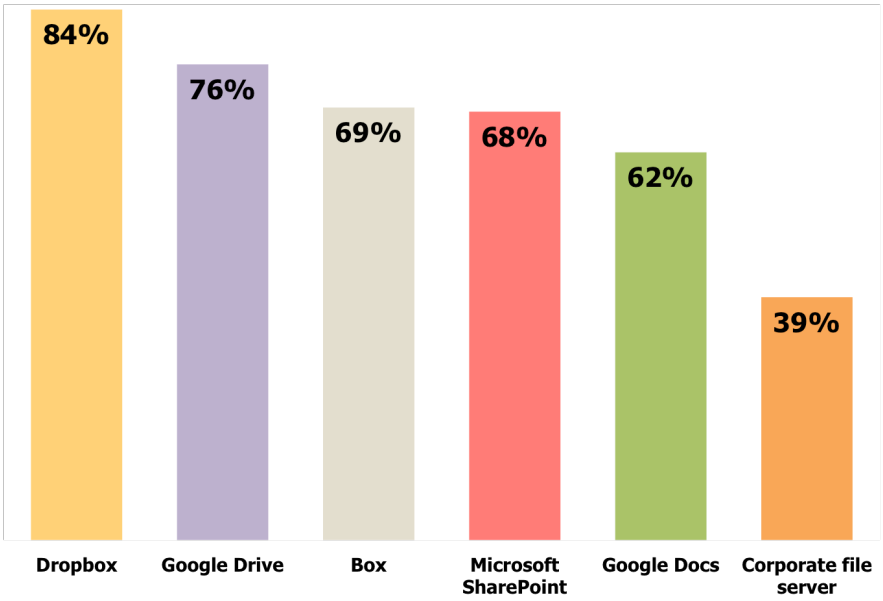
Other Osterman Research surveys have found that file sync and share tools are widely used in organizations of all sizes, and that most of these tools are deployed by individuals independently of any sort of "blessing" from their IT department. Moreover, the vast majority of employees use these tools because of their utility in making employees more productive, giving them access to files when they are working from home or traveling, and for backup purposes. It is important to note that the vast majority of employees deploy these tools for "good" purposes: to enable them to have access to files when they are out of the office or when working from a mobile platform, for example.

## MOST CONTINUE TO HAVE ACCESS EVEN AFTER THEY HAVE LEFT THEIR PREVIOUS EMPLOYER

Our research also found that a large proportion of users continue to have access to these services and content repositories even after they leave their previous employers. For example, as shown in Figure 2, almost all of the users who employed Dropbox in a previous job continue to have access to the content stored within their Dropbox account in their current job. Similarly, we also found that for the other services noted in the figure above – with the exception of corporate file servers – most employees continue to have access to their previous employers' content.

***68% of information workers store work-related information in a personally managed file-sharing solution.***

**Figure 2**
**Percentage of Employees Who Continue to Have Access to Systems They Used With a Previous Employer, by Platform**




*Source: Osterman Research, Inc.*

## MOST STILL HAVE ACCESS TO OTHER CORPORATE DATA REPOSITORIES

In addition to the platforms noted above, users continue to have access to a wide range of accounts, IT services and platforms that they used when working for a previous employer. For example, 24% of users still have access to a PayPal account they used when working for a previous company, 21% have access to Facebook and 18% have access to LinkedIn. In all, we found access to at least 38 different systems that employees used when working for a previous employer across all of the surveys conducted, although the per-employee figure is lower than this in most cases.

Amazingly, when analyzing all of the applications to which employees still have access, 89% of employees continue to have access to at least one application from their former employer now that they are working for someone else.

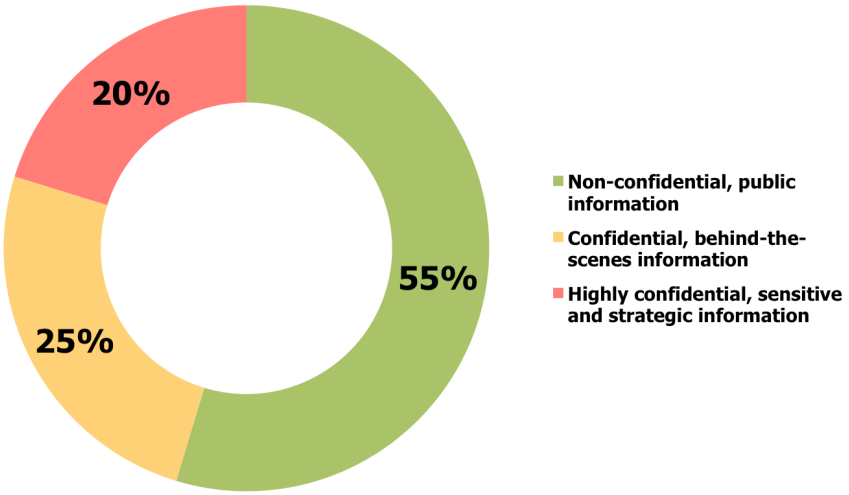
Another survey conducted by Osterman Research found that a wide range of applications are used by employees – an average of nearly 15 major applications, including corporate email, archiving and compliance solutions, mobility solutions, real-time communications, security, telephony, etc. This illustrates the extent of the fundamental problem: there are many venues in which employees store corporate data, only some of which are readily accessible to their IT department or others charged with managing corporate data.

## MUCH OF THIS DATA IS SENSITIVE

Our research also found that a significant proportion of the data to which employees have access from their previous employment is either confidential or sensitive. As shown in Figure 3, one-quarter of the data that employees can access from a previous employer is what they would consider to be confidential and non-public data. Another 20% of the data is content that these employees would consider "highly confidential, sensitive and strategic".

***89% of employees continue to have access to at least one application from their former employer now that they are working for someone else.***

**Figure 3**
**Sensitivity of Data From Previous Employers' Accounts to Which Employees Still Have Access**




*Source: Osterman Research, Inc.*

This represents a critical problem for organizations, as discussed later in this white paper, since it means that a large proportion of intellectual property, customer information, sensitive employee information and other content that should be controlled is not managed appropriately.

## MOST EMPLOYERS DO NOT ADDRESS THE PROBLEM

One of the more surprising issues that came out of the research is the fact that most employers did not request login information from employees when they left their previous job. Our research found that 60% of the ex-employers of those we surveyed did not request the login information for the cloud applications that employees were using.

In most cases, this is not due to negligence or carelessness on the part of an IT department or the managers who were previously responsible for these employees. Instead, it represents a couple of important issues that organizations need to address:

- The larger problems associated with the Bring Your Own Device (BYOD) and Bring Your Own Applications (BYOA) phenomena that many organizations still are not addressing properly.

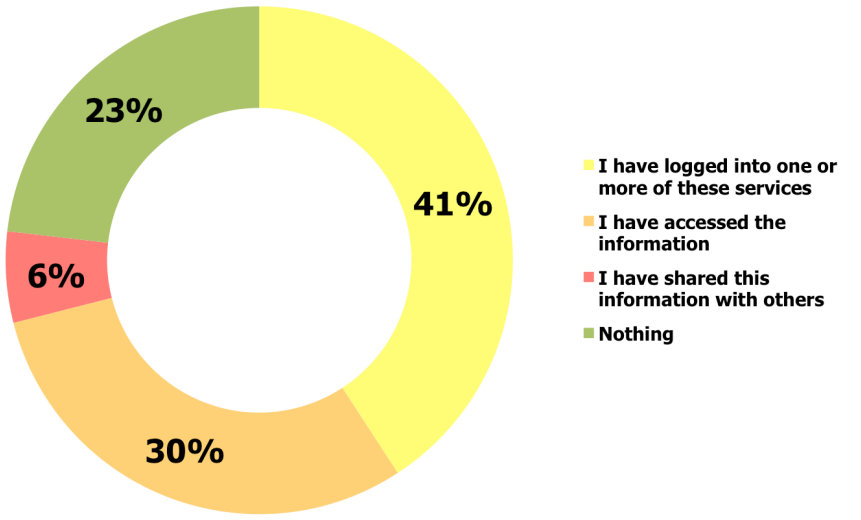
- In many organizations, the responsibility for decommissioning employee access to various applications may not be clearly defined as being the responsibility of the IT department, the employees' manager, HR or some other group.

## WHAT DO USERS DO WITH THE DATA?

We also asked employees who had access to data from their previous employers what they did with this information. As shown in Figure 4, nearly one-quarter of employees did nothing with the information even though they still have access to it. However, two in five employees have logged into one or more of the services to which they still have access without viewing the information or using it in some manner. Another 30% have actually accessed the information, and one in 16 have actually shared this information with others.

***A large proportion of intellectual property, customer information, sensitive employee information and other content that should be controlled is not managed appropriately.***

Figure 4
"What have you done with the information from your previous employer to which you still have access?"




*Source: Osterman Research, Inc.*

## THE IMPLICATIONS OF ROGUE APPLICATIONS

One of the fundamental problems with letting ex-employees have access to corporate data is the organization's loss of control over potentially sensitive or confidential content. The implications and possibilities that can result can be damaging and wide-ranging:

- **Violations of data breach statutes**
  Organizations have a variety of regulatory and other obligations to protect and control access to certain types of data, such as employees' health information or customers' financial data, from unauthorized access, including access by ex-employees. Forty-six of the 50 US states have data breach notification statutes that require parties whose data has been breached to be notified about the unauthorized access or loss of data. As just one example, New York's State Technology Law reads in part:

  - "Breach of the security of the system shall mean unauthorized acquisition or acquisition without valid authorization of computerized data which compromises the security, confidentiality, or integrity of personal information maintained by a state entity."

  - "In determining whether information has been acquired, or is reasonably believed to have been acquired, by an unauthorized person or a person without valid authorization, such state entity may consider…indications that the information has been downloaded or copied."

  The consequences of a data breach can be significant: expensive notification and remediation activities, such as the purchase of credit reporting services for affected customers; loss of revenue from customers who no longer want to do business with a firm that has lost their data; negative press reports; and damage to corporate reputation from customers and prospective customers who view the organization's IT policies as lax.

*The consequences of a data breach can be significant.*

- **Violation of regulatory compliance requirements**
  There are a variety of federal and state regulations that obligate organizations to protect sensitive or confidential data. For example, the Safeguards Rule within the Gramm-Leach-Bliley Act (GLBA) obligates financial institutions to adequately protect their clients' data. The Florida Information Protection Act of 2014 (FIPA) requires notification of affected individuals as with other data breach statutes, but expands what is considered "personal information", expands the state's investigative authority, and implicitly requires every organization in Florida to develop a written policy focused on data security.

  Typically, these requirements obligate organizations to protect content from unauthorized access. Ex-employees with unfettered access to sensitive or confidential data clearly constitute such unauthorized parties.

- **An inability to satisfy eDiscovery obligations**
  Organizations that do not have full and ready access to all of their discoverable content face the prospect of being unable to satisfy electronic discovery orders. This can put an organization into the unenviable position of telling a judge that they cannot find all of their relevant content or that they cannot access it and, in some cases face an adverse inference instruction that allows jury members to assume that a failure to produce content can be considered evidence of culpability.

- **A failure to fully implement legal holds**
  Similarly, organizations that do not have full access to their content cannot place this data on legal hold if and when required to do so. This means that relevant content, such as files stored in Dropbox, is subject to deletion by former or current employees, allowing information to be lost in violation of legal requirements to retain it.

- **Loss of data**
  Employees with continuing access to corporate data after they leave a company can inadvertently or intentionally delete data that might be useful to their former employer. For example, an employee who used a personal Dropbox account to sync and share work data might delete his or her previous employer's data simply to make room in his account for new content, rendering the data permanently unavailable.

- **Loss of intellectual property**
  When data is stored in repositories that are outside the control of IT – or, worse, accessible by non-employees – there could be a loss of intellectual property in the form of spreadsheets that contain financial information, presentations with marketing plans, engineering drawings, or other sensitive or confidential information. In some cases, organizations can even lose their patent or trademark rights over this content.

- **Potential alteration of data**
  Data that is accessible by former employees could, in some rare cases, be altered or sections of it deleted for any of a variety of purposes. While not a common problem, there are situations – such as during investigations or legal actions – in which content might be modified. For example, in one case, a former IT specialist altered and removed a number of documents that were harmful to the governor of Georgia[1].

- **Actions of malicious ex-employees**
  There are situations in which ex-employees may act with malicious intent, particularly those who have been terminated. An employee who wants to harm his or her previous employer could access corporate data and provide it to competitors, post it on a public forum, delete important information or alter

***Employees with continuing access to corporate data after they leave a company can inadvertently or intentionally delete data that might be useful to their former employer.***

[1] http://chronicle.augusta.com/news/metro/2013-10-09/across-region

records. Disgruntled ex-employees with access to previous employers' social media accounts could damage the reputation or brand of the latter quite easily. While not common, this is a definite possibility that employers need to consider.

## WHAT SHOULD YOU DO?

The problems discussed in this paper are quite serious and correcting them should be a top priority for any organization. Osterman Research recommends a multi-step approach in dealing with these issues:

### UNDERSTAND THE SCOPE OF THE PROBLEM

Before doing anything else, decision makers should understand how much of a problem they face. IT should undertake a concerted effort to explore what applications are in use by employees, where corporate data is stored, and why various tools are employed. Exploring these issues might involve user surveys, network scanning or discovery tools that can find every known source of corporate data.

### ASK EMPLOYEES FOR THEIR LOGIN CREDENTIALS

Employers should do something that most of them are not doing: ask departing employees, as well as those who are staying with the organization, for the login credentials to all of the repositories that might contain corporate data. This might seem like an obvious thing for employers to do, but they are not doing it and should be. We would go even further and ask not only for login credentials, but ask employees to sign a statement upon their departure that a) they have turned over all login credentials and revealed the locations of all corporate data to which they have access, b) that they will not access corporate data after they have left the company, and c) that if they come across sources of data about which they had forgotten they will immediately inform the company.

***Employers should do something that most of them are not doing: ask departing employees… for the login credentials to all of the repositories that might contain corporate data.***

### ESTABLISH POLICIES ABOUT APPROPRIATE USE

Another essential element in protecting corporate data from the problems discussed in this paper is the creation of acceptable use policies for every application type that might house corporate data. For example, the policy should specify if and how file sync and share tools, cloud storage, personal Webmail and other tools can be used. These policies should specify the tools that can and cannot be used, what types of data they can store, that IT must be given access to the corporate content stored in them, and that employees will not access data once they leave the company.

### CENTRALIZE ACCESS TO CLOUD APPS VIA A SINGLE SIGN-ON (SSO) PORTAL

One way to make it more difficult for employees to maintain rogue access to applications is by implementing an IT-managed SSO portal that will enable access to all applications. Combined with a policy of using only very strong passwords for individual applications and the SSO portal, this will reduce the likelihood of employees gaining rogue access to applications upon their departure simply because they're less likely to remember them. While this won't stop malicious employees from gaining access to corporate applications after they leave, it will stop a good deal of accidental data leakage.

### OFFER GOOD ALTERNATIVES

Osterman Research also recommends that IT offer good alternatives to the tools that employees have deployed. For example:

- If employees want to use the standard version of Dropbox in order to have access to their corporate files while traveling or working from home, the company should offer an alternative that will be just as easy to use, but that will enable IT to have access and control over corporate information.

- Instant messaging (IM) and real-time chat tools offer employees the ability to communicate more quickly and more efficiently than they can with email in many cases. However, consumer-focused tools do not permit content to be archived or otherwise managed by IT. Replacing consumer IM and chat with enterprise-grade equivalents can enable organizations and employees to achieve the best of both worlds: ease of communication and IT control over corporate content.

- Many employees use personal Webmail for work purposes, sometimes as a backup for instances in which the corporate email system goes down or when they need to send files larger than the corporate email system will permit. If an organization were to provide a backup email capability or a file-sharing capability for large files that kept IT in control, here again the best of both worlds could be realized.

The bottom line is that for just about every "consumer" app or cloud service that employees will want to deploy there is a better alternative that will satisfy the needs of both employees and the data protection requirements of the organization.

***For just about every "consumer" app or cloud service that employees will want to deploy there is a better alternative.***