Intralinks® Survey Report

Safe Sharing: A Survey of Enterprise IT Decision Makers on Best Practices for Adopting File Sync and Share Applications

New research conducted by Harris Poll

June 2014

Executive Summary

The file sync and share (FSS) market has generated tremendous momentum, with an estimated 300 million-plus global users.

The main reason for this broad-based adoption is that FSS fills a basic need for almost anyone – they make personal files available anytime you need them, from any device. Another cause of the rapid growth of FSS users has been the "freemium" business model adopted by some of the leading vendors. While this approach has been successful at encouraging millions of consumers to subscribe to these services, it has introduced a new problem for many enterprises. That's because the use of free FSS services by employees represents an unmanaged channel for potential information leaks. Subsequently, many enterprises put consumer FSS services on their "black list" of forbidden applications.

Freemium FSS has written a new chapter in the bring-your-own-device (BYOD) saga, one that we can title: "Bring-your-own-Cloud (BYOC)." Personal cloud services, such as FSS, give employees an easy way to store business documents beyond the confines of corporate IT — raising obvious security and compliance challenges. This is compounded by the sync function, where files stored in the cloud may be synced to any number of personal employee devices (laptops, tablets, smartphones, etc.).

To understand the impact of a freemium FSS business model on enterprise IT departments, Intralinks sponsored an online survey conducted on their behalf by Harris Poll in April among 308 IT professionals. All of them indicated that they are either the sole IT decision makers in their organizations, or hold major influence over IT decision-making. The survey sought to understand current opinions about freemium FSS services, and the technical requirements for deploying FSS in the enterprise.

FSS Security Concerns:

31%

of IT decision-makers trust using FSS apps for sharing personal financial information.

38%

trust FSS apps for sharing work files outside the firewall.

46%

agree "Data is leaking from my company due to unmanaged use of file-sharing products."

84%

agree the adoption of free FSS products by employees creates a potential security problem.

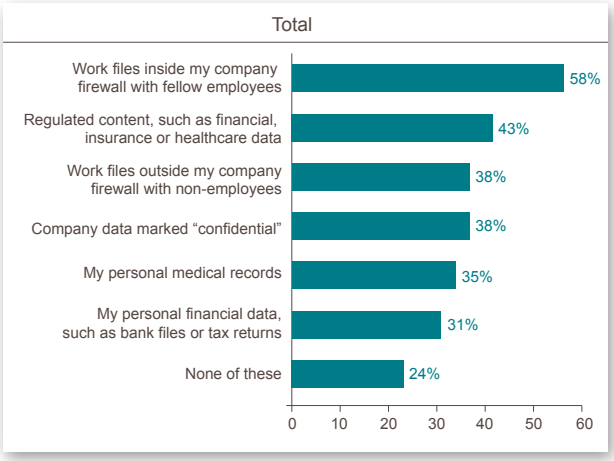
Enterprise IT Perceptions of Freemium FSS Security

Most people don't think like adjusters at an insurance company – psychologists have long understood that we perceive risks emotionally and qualitatively, not rationally and objectively. And when it comes to the relative risks of using FSS, this fact becomes quite obvious.

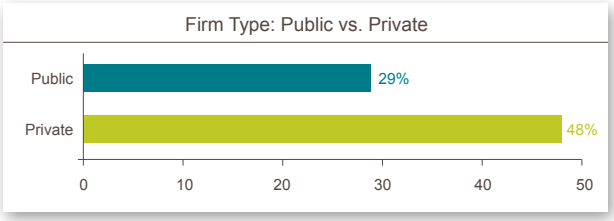
We asked survey respondents how comfortable they felt sharing various types of information on these services. Predictably, these decision makers expressed greater confidence in sharing files inside the firewall with fellow employees, as compared to outside the firewall with non-employees. Interestingly, respondents also showed a greater propensity to share work information than they would their own personal financial or medical information. (This also provides some worrying insight into how employees assign risk in their own lives.)

Typically, the perception of risk relates to perceived immediate personal consequences, so sharing a tax return feels riskier than sharing confidential company files. (Again, this is bad news for enterprise IT personnel entrusted with protecting corporate assets.) Notably, almost one in four IT decision makers would not share any of the indicated file types over freemium FSS vendor services.

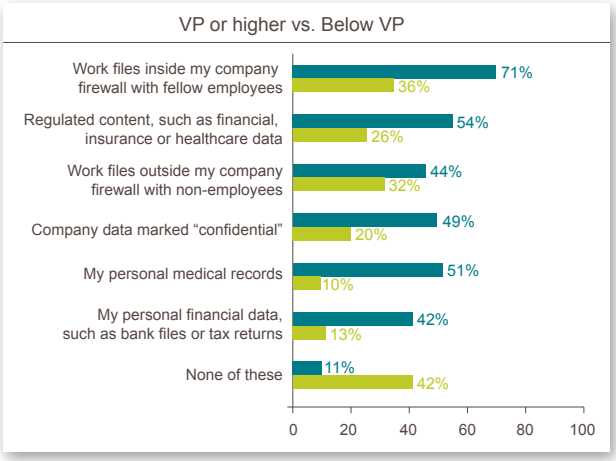
Which of the following information, if any, would you trust file sharing apps like Box or Dropbox to share?



As might be expected, public company respondents showed significantly more reluctance than those in private companies to share regulated content across freemium FSS vendor services. Fewer than one in three public company respondents indicated they would feel comfortable sharing such information.



IT decision makers with a title of vice president or above were actually more likely to share sensitive company and personal information than were thosewho were below vice presidents. This proclivity makes it likely that there will be unauthorized access to sensitive information, and suggests more needs to be done to educate business leaders about the risks of file sharing. Not surprisingly, younger people were more likely to risk sharing sensitive information over freemium FSS vendor services than older people.



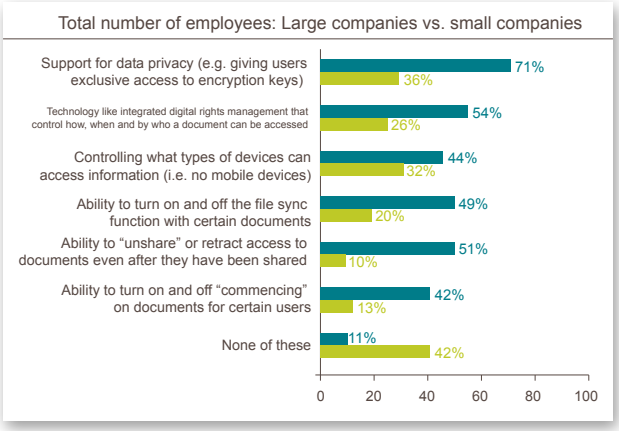
Enterprise Requirements for FSS Applications

The “consumerization of IT” trend is real. It has led to the broad adoption of smartphones in enterprises, and has also changed the look and feel of business software. Today, business employees expect their applications to be as intuitive and easy to use as consumer applications – these expectations have caused this fundamental shift.

However, in the context of freemium FSS applications, consumerization takes on a new context. This is due to the incredibly low barriers to adoption, and the security and compliance requirements of enterprises. Freemium FSS apps offered by vendors like Box and Dropbox are easy to use, and they meet the most common consumer use-case: to share “stuff” easily with other people. Enterprises, however, require control over how files are accessed and shared, which is why freemium FSS vendors’ services are often blacklisted by enterprise IT organizations.

To understand enterprise requirements for FSS, the survey asked respondents to identify which technical features are required for the adoption of FSS. The most commonly cited features included: support for data privacy; end-user device access control; and integrated digital rights management (DRM).

Which of the following features of file sync and share are mandatory at your company?



Among respondents from large enterprises (more than 250 employees), the “ability to turn on and off sync” became the third most commonly cited required feature. This is logical because sync creates security and compliance risk by enabling automated distribution of company information across end-user devices. Additionally, larger companies tend to have more complex security and compliance requirements. Large company respondents also more likely to indicate a mandate for nearly all of the security and management features listed in the question than did their small-company counterparts.

Enterprise View of Freemium FSS Business Model

Eighty-four percent of survey respondents said they have concerns about data privacy with freemium FSS vendor products. However, this concern became even more pronounced when respondents were presented with the prospect of users intermingling personal and professional file-sharing activities.

Dropbox has adopted this approach with Dropbox for Business, where people can access both their personal and business accounts through a single login. Eighty-eight percent of executives agreed that allowing users to access both their private and business file-sharing accounts from the same login poses a security threat. Even after removing the "single login for both accounts" dynamic, almost as many (84 percent) agreed that allowing users to have both their private and business files shared from the same FSS product poses a potential security threat.

When you think of file sync and share products like Box and Dropbox, how much do you agree or disagree with the following?

Summary of Strongly/ Somewhat agree

84%

I have concerns about data privacy when I use file-sharing products like Box and Dropbox

77%

The financial viability of file-sharing companies like Box and Dropbox in a key criterion when I consider a technology purchase

How much do you agree of disagree with each of the following statements regarding security and privacy?

Summary of Strongly/ Somewhat agree

88%

Allowing users to access both their private and business file-sharing accounts from the same login poses a security threat

81%

Allowing users to have both their private and business files shared from the same file-sharing product poses a security threat

51%

Even if a product has been blacklisted by other companies, I am still willing to consider using it at my company if the solution can cost-effectively solve a problem

The freemium business model also appears to create some biases among IT decision makers about vendors. Only 51 percent of IT decision makers agreed that they would be willing to consider using an FSS product that was blacklisted by other companies. Additionally, 77 percent agreed that financial viability is a key criterion when considering a technology purchase. This number spiked to 85 percent among those with a title of vice president or higher.

Recommendations

Freemium FSS services are extremely popular with consumers for good reason: they are easy to use; they meet an ubiquitous need; and, of course, they are free. What this means for enterprises is they are not going to go away. Today, it is Box and Dropbox; tomorrow, it could be other vendors with different schemes for enabling people to share "stuff" with other people. This also means that IT professionals cannot ignore the security and compliance risks these services represent. Instead, they need to develop strategies for adopting FSS functionality within the context of their own management, security and compliance requirements. Simply blacklisting products without endorsing an acceptable alternative will only impair employee productivity, and in any event is likely to be circumvented. In selecting a secure and compliant FSS solution, consider the following:

- **Understand data-sharing needs and use cases.** These will be wildly divergent, based on employee roles. A finance director sharing company financial information with auditors, for example, has different requirements from a salesperson sharing marketing brochures, presentations and videos. Understanding the range of use cases helps to inform the product features needed to meet security and compliance requirements.
- **Never lower your standards.** As mentioned earlier, freemium FSS services are very popular because they are easy to use. The problem for enterprises is that these services often do not meet security and manageability standards. When considering FSS solutions, relaxing corporate security standards in favor of employee usability is a recipe for disaster – so it is important to be disciplined and maintain those standards when evaluating solutions.

With these considerations in mind, there are multiple steps IT professionals can take to solve the freemium FSS problem:

- **Put the end-user first.** Adoption is the goal, so focus first on what users want. To achieve acceptance, your solution needs to be easy to use and simple to provision and deploy.
- **Keep lifetime control of documents.** Accept the reality of the "Firewall Fallacy" – that is, the belief that building an enterprise fortress will protect data. Make sure that even if a file is shared outside the firewall, it always remains completely inside your control. Security must travel with the file, and next-generation information rights management helps make this possible. Having lifetime control, so that a file can be revoked at will, or at a predetermined time, is a critical requirement.
- **Move beyond sharing.** FSS is a feature, not a complete solution. Effective collaboration requires far more than the sharing of documents. Your enterprise teams need to be able to work collaboratively on information in simple work streams, while easily managing tasks and roles.
- **Build on your existing and proven solutions.** Collaboration solutions should work with key applications that might already be running in your network, such as Microsoft SharePoint. This is a sound economic decision and will encourage adoption, as it supports existing processes and workflows.

- **Prepare for upcoming regulatory requirements.** Work with your legal and security teams to fully understand the regulatory environment. Make sure that existing collaboration practices are fully compliant.
- **The "Snowden Effect" is real.** Data privacy is perceived as a growing issue, and many countries and jurisdictions are placing restrictions on where data can be housed and where it can travel. Think about the kinds of data you share, or where you conduct business. Be aware of the complexities and costs associated with different data deployment options. Understand how new technologies, such as customer-managed encryption keys, can give you sole access control to unencrypted data.
- **Educate your employees.** Teach your people about the risks of business data loss or theft. But also instruct them about best practices for keeping their personal data safe, too.

Survey Methodology and Respondent Profile

Between April 2-11, 2014, Harris Poll fielded a survey to 308 IT decision-makers on behalf of Intralinks, Inc. "Decision-makers" were defined as full-time IT employees who indicated they had either sole or "major" influence over purchasing decisions in their organizations. One hundred and fifty-one of the survey respondents were from companies ranging in size from 20 to 249 employees. One hundred and fifty-seven were from companies with 250 or more employees, and all were based in the United States. One hundred and ninety-three respondents held a title of vice president or higher. For a complete copy of the survey and respondent profiles, please email securecollaboration@intralinks.com.