Whitepaper:

File-sharing and sync done right

GFI MailArchiver™

Archiving for productivity, management and compliance

Contents

Risks of sharing 3

The need to share 5

Don’t just say “No” 6

Compliance 8

Location, location, location 9

To cloud or not to cloud? 10

The dos 11

The don’ts 11

Archiving to the rescue 12

GFI MailArchiver®2014:
A complete file and email archive solution 13

About GFI Software 15

Hosted shared storage systems sound like an end user's dream come true. For little or no money, it's possible to store any files in the cloud, and share them with friends and colleagues.

This approach is fine for non-critical items. However, these services are now being used to store and share critical business data. The problem is consumer-grade file sharing and synchronization tools are not nearly secure enough to handle truly important pieces of information. Such services lack the proper management tools.

If you don't think it's much of a problem, ask yourself these questions (and remember that files belonging to you and your company are out there somewhere on insecure cloud file-sharing services):

- Do you know where your files are located?
- How many other users are sharing the same servers?
- Exactly what kind of security is applied?
- Are there strong access controls?

A smart approach is to assume the answers to those questions is "No."

> "Heartbleed was unprecedented in scale. Countless reports said it affected roughly two-thirds of websites."

Risks of sharing

So what can go wrong? Plenty. Let's take the easiest route to trouble: You have end users who apply proper passwords to their file sharing application, and even change it regularly. Their accounts were never compromised, but the confidential files they stored were leaked by other people that had access. And these individuals likely have access to a good deal of your shared files. Even though you thought you did everything right, the data was compromised anyway.

Tougher to pull off, but not really all that difficult, is having a hacker crack the password. Users, struggling to keep track of their passwords, tend to reuse passwords. So if a hacker learns the email password (which can be as simple as "password123"), he or she now can get into LinkedIn, Facebook, and shared file services. Who knows what kind of damage that access can cause?

With consumer-grade tools, the passwords are only as good as the end user that picked them. There are all kinds of ways to crack these protections and gain access to end user files as well as shared company content. Social engineering can reveal these passwords. Perhaps more prevalent, a hacker can gain access to a user's email account, and then find the same password used to secure other services. Mobile devices can be particularly vulnerable to password theft.

> "Users, struggling to keep track of their passwords, tend to reuse passwords"

Data leakage may be the least of it. Identity theft and crimes committed in your name are other possibilities. And if any of the information is embarrassing, blackmail is even a possibility. Don't think it can happen to you? A survey by Fiberlink and Harris Interactive found that more than half of the U.S. workers surveyed use personal tablets and smartphones for work. Here's the scary part: One-quarter of the respondents open or save work documents in their third-party apps such as iCloud or Dropbox, and 20% paste work data into their private email systems.

The need to share

There are 300 million estimated worldwide users of file synchronization and sharing (FSS) tools. So why is it so popular?

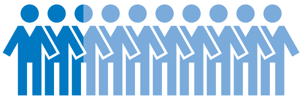
"There is a growing need for users to share content and collaborate with other employees, business partners, consultants and clients. While email is the primary tool for sharing content in most organizations, it has serious limitations that FSS tools have helped users to overcome," says the Osterman Research report File Synchronization and Sharing Market Forecast.

But Osterman also points to what it calls "serious problems with current FSS tools," going on to say:

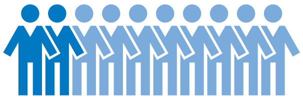
"Many of the free or low cost, cloud-based tools provide robust functionality, but are seriously lacking in enterprise-grade features. A serious shortcoming of most FSS solutions is that they provide IT with little control over the lifecycle of data. Moreover, corporate policies that manage encryption, backup, archiving or DLP for content sent through email or FTP systems cannot be applied to content sent through most FSS tools.

"In short, the lack of IT control over the content sent through most of these tools puts the employee in charge of employer-owned data, when in reality the opposite should be true. The proportion of Dropbox deployments under control of individual employees – and not IT – increases with the size of the organization."

Consumer-grade services in the cloud are not the most reliable things ever built. In fact, DropBox dropped service

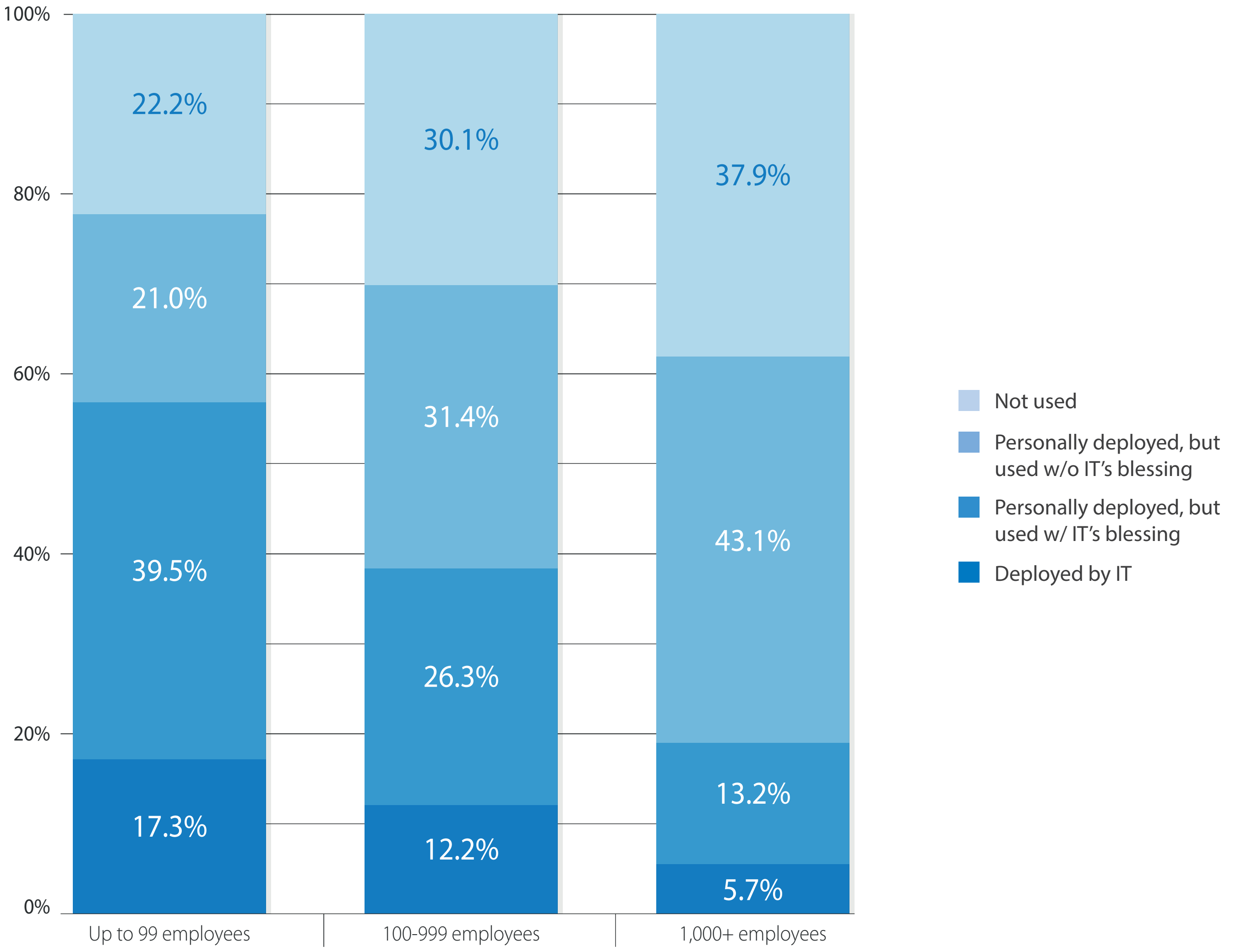


One-quarter of the respondents open or save work documents in their third-party apps such as iCloud or Dropbox.



20% paste work data into their private email systems.

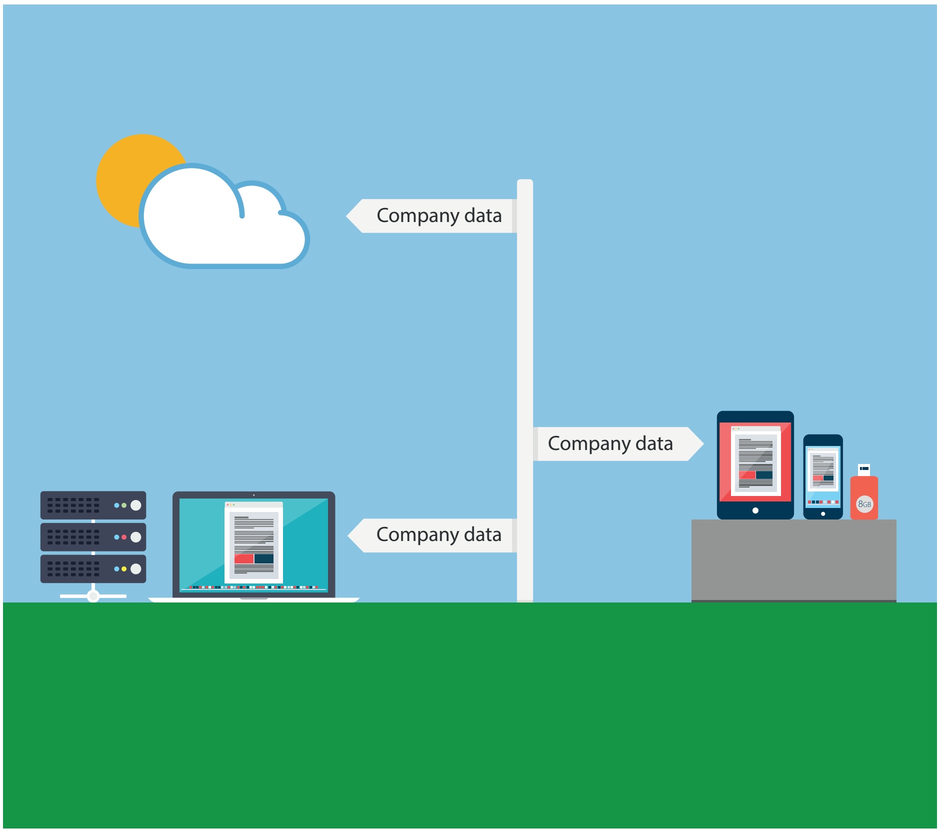
for three days for many customers after an operating system upgrade went wrong. At first, the reason for the outage was murky, with speculation pointing to a hack attack after the bad guys claimed credit and DropBox dragged its feet for hours setting that record straight. Of course, if this was an IT service that went down in your company, you'd know pretty fast what the problem was. The best answer is to replace vulnerable file-sharing systems with safe, business-class tools.



Don't just say "No"

Just saying "no" to shared storage/file synching and shared services is not always a wise idea. What they offer is too compelling as they let employees work from anywhere on the files and folders of their choice. Aside from security issues, this is not inherently a bad thing.

It is employees who are taking the initiative to be more productive, accessible and able to do their jobs in a way that satisfies their employer, partners and themselves (as it allows them to work from home comfortably). And these services can be far better than putting critical company files on a USB memory stick, which is easy to use but also easy to steal.



> “
> It is employees who are taking the initiative to be more productive, accessible and able to do their jobs in a way that satisfies their employer, partners and themselves.
> ”

This convenience is even more important for road warriors, who are now using these services for backup, in addition to file sharing and access. If a file goes missing on one machine, it is easy to find on the public cloud access site. And if a laptop is lost, stolen or suffers a catastrophic crash, many files are still available.

Furthermore, a few cloud file sharing services can cost a fraction of a typical Microsoft® SharePoint® install, with far less complexity and a faster time to increased productivity. However, since file sharing solutions also support collaboration, this certainly includes ad hoc collaboration.

These are often "Shadow IT" projects – tasks done without explicit IT knowledge or support. It may be that multiple file sharing tools and services are in use at the same time. And some of these may be paid services that require proper approval, as they impact the company's bottom line.

Another problem is that these tools are not built for safe, long-term storage of your data. File sharing is great, but file sharing with a full ability to archive content is even better.

Of course, chances are you couldn't stop file sharing and sync even if you wanted to. The market is too big and growing too fast.

"Osterman Research forecasts that the worldwide Total Available Market (TAM) for FSS capabilities was 591.4 million seats in 2012 and will grow to 781.4 million seats by 2017, achieving a compound annual growth rate of 5.7%," the market research house said.

> "Instead of fighting file sharing, IT should offer a way to do it better with supported business-class tools."

Instead of fighting file sharing, IT should offer a way to do it better with supported business-class tools that are secure, flexible and scalable, and capable of providing a true archive.

Compliance

Not all companies are required to meet compliance regulations such as Sarbanes-Oxley (SOX) or the Health Insurance Portability and Accountability Act (HIPAA). But it is never a bad idea to act like such legislation applies to your business. After all, compliance rules basically require that data is secure and protected.

If your company must meet legal and regulatory standards, allowing your data to be out on Box, Dropbox, or OneDrive can create serious liabilities – with possible fines of thousands or even millions of dollars.

You likely require a higher level of security, whether compliance is an issue or not. If you have data in the cloud, make sure it is strongly encrypted for peace of mind, especially when you consider several high-profile hacks of supposedly secure cloud providers.

A better approach is to keep your files local through an archive on your own servers and disks.

“One of the main concerns of the IT admins is the location of the data.

In many cases, there are laws and regulations detailing the level of auditing and control on who can access data and from where.”

Location, location, location

IT admins are not just responsible for keeping systems up and running – they must also ensure the safety and integrity of the data under their watch. That said, one of the main concerns of the IT admins is the location of the data. In many cases, there are laws and regulations detailing the level of auditing and control on who can access data and from where.

Storing your data in-house means you always know where it is located, how it is being managed, and what types of backups are in place.

“Most cloud-based FSS providers do not allow their customers to control the physical location of data storage. This can lead to regulatory problems or other issues in jurisdictions that require sensitive data to be stored only in certain geographies,” Osterman Research says. "For example, a non-US company will typically prefer that its data not be stored in a US-based data center in order to avoid its access under the Patriot Act."

To cloud or not to cloud?

Many products in this space are so-called Cloud File Sharing (CFS) tools, and they can be considered a low-end form of Software-as-a-Service (SaaS). According to research by Frost & Sullivan's Stratecast division, more than 80% of employees use rogue SaaS services at work. Ask IT the same question, and the percentage is even higher.

And these apps aren't going away anytime soon. Frost & Sullivan sees the SaaS market growing at a CAGR of 16%, and poised to hit $23.5 billion in 2017. This dramatic growth creates equally dramatic problems, including data leakage, security, compliance issues and availability.

$

Frost & Sullivan sees the SaaS market growing at a CAGR of 16%, and poised to hit $23.5 billion in 2017.

It is also the case that SaaS, or having applications and files in the cloud, isn't always the best answer. IT doesn't have control of the software and, more troubling, has no idea where the data actually resides. With cloud solutions, the power and control are taken away from IT. With on-premise tools, IT has a stronger sense of security knowing it can audit and control access to the data and applications.

This is particularly true for file sharing and sync, Osterman Research says:

"When content is stored in an FSS vendor's data center, accessing it for purposes of eDiscovery or a regulatory audit becomes impractical or impossible because IT must gain access to every account and then search it, assuming they are even able to do so. Moreover, tools like Dropbox are not compliant with a number of compliance standards like HIPAA, PCI DSS, ISO 27001, ISO 9001 or the Family Educational Rights and Privacy Act (FERPA)."

The dos

Do run an inventory of what end user software is installed and what web services are in use. Block services you don't consider safe.

Do make shared storage and FSS part of your security and acceptable use policies.

Do evaluate tools that allow for proper storing and sharing of files.

The don'ts

Don't allow the use of commercial grade file share and sync software. Instead, provide a robust solution that meets your security needs – and train end users to operate it.

Don't think you are in compliance because your internal systems and storage are in compliance. Data leaks and privacy breaches more often come from unauthorized apps or services.

Don't let end users mix their personal files with work data, especially when stored in the cloud. The temptation is to share the personal stuff, such as photos, but this gives easy access to your company's private data:

"Another problem with the use of many FSS tools is that they can be used to send and share a mix of corporate and personal content because employees are in charge of their management, not IT. For example, mixed with sensitive company information might be an employee's personal photos, resumé, recipes or personal tax returns," Osterman Research says. "This not only makes activities like eDiscovery or regulatory compliance more difficult because reviewers must sort through personal data as they search for corporate records, but it raises the often onerous issue of employee privacy rights."

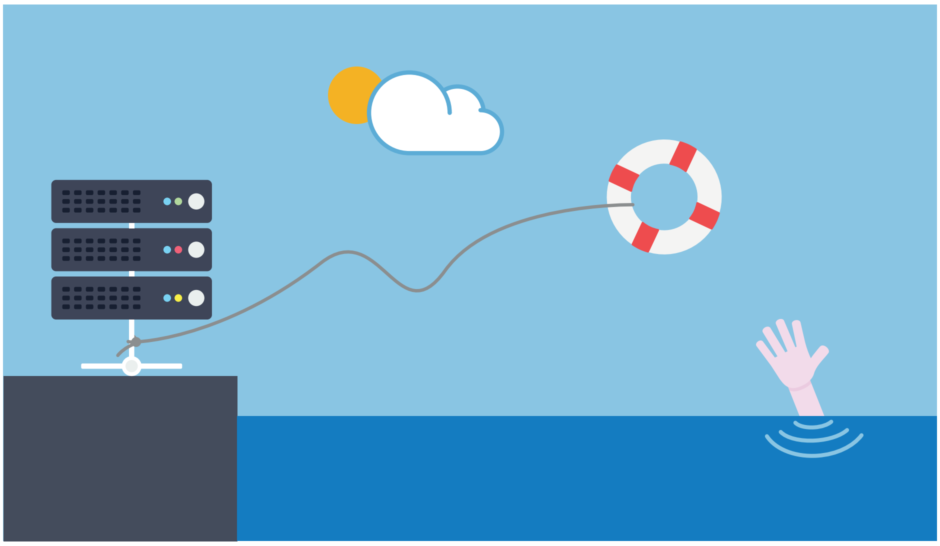
Archiving to the rescue

Any company that takes the IT business seriously has to move away from consumer-grade tools.

> "Any company that takes the IT business seriously has to move away from consumer-grade tools."

Osterman Research recommends "the deployment of an enterprise-grade FSS capability as a replacement for non-enterprise tools."

Doing so will offer users the flexibility and ease of use that drives them to the current crop of cloud-based FSS tools, and it will give IT the control over corporate content that is sent by and stored in these systems, the Osterman FSS report says.



Archiving is one way to bring discipline to the process of storing and managing these files. You can decide how long the files are stored, who can access them, and how they are secured.

GFI MailArchiver® 2014: A complete file and email archive solution

The answer to FSS problems is to give your end users a better option and get them to use it. For instance, GFI MailArchiver 2014 – with its File Archive Assistant (FAA) – now offers file archiving that works precisely the same way it handles mail.

By using GFI MailArchiver, you gain sharing and archiving features without needing a third party to actually store the data, thus avoiding the possibility of your data being lost or leaked. Instead, these files are safely backed up, simple to restore, and because they are in an archive, they are easy to search.

With cloud-based storage and sharing services, you either lack the ability to audit, or you are fully dependent on the limits of the auditing features provided. With GFI MailArchiver, auditing is enabled out of the box, and can use solutions like GFI EventsManager® to monitor for important events – both those that should and should not occur.

Archiving satisfies a critical business need. Chances are your company relies upon presentations, reports, spreadsheets, and key Word documents, all of which constitute much of your business intelligence. But how do you store, track and use all this information? Using ad hoc methods is hugely time-consuming and ineffective.

By using GFI MailArchiver, you can:

- Use search to quickly find and access the right files.
- Connect all employees globally, enabling them to share files and cooperate on projects – no matter what device they are using.
- Meet compliance standards by properly retaining files and having an audit trail.
- Maintain critical business intelligence in a single archive that is secure, backed up, searchable and compliant. And you can control this data as long as you want.

With GFI MailArchiver, you'll always have the right version of a file, even if it's shared. All changes are saved, and the history of file revisions is kept so you can return to a previous version. Meanwhile, two types of file sharing are supported. A single user with multiple devices can keep documents in a common central archive that is regularly synchronized. And co-workers can share files through a shared GFI MailArchiver location.

Try GFI MailArchiver 2014 today for a free 30-day trial.
http://www.gfi.com/mailarchiver

Other network security solutions from GFI:
GFI EndPointSecurity
GFI EventsManager
GFI WebMonitor

About GFI Software

GFI Software™ develops quality IT solutions for small to mid-sized businesses with generally up to 1,000 users. GFI® offers two main technology solutions: GFI MAX™, which enables managed service providers (MSPs) to deliver superior services to their customers; and GFI Cloud™, which empowers companies with their own internal IT teams to manage and maintain their networks via the cloud. Serving an expanding customer base of more than 200,000 companies, GFI's product line also includes collaboration, network security, anti-spam, patch management, faxing, mail archiving and web monitoring. GFI is a channel-focused company with thousands of partners throughout the world. The company has received numerous awards and industry accolades, and is a longtime Microsoft® Gold ISV Partner.

CDT130 jul14

www.gfi.com

For a full list of GFI offices/contact details worldwide,
please visit: www.gfi.com/contact-us

Disclaimer. © 2014. GFI Software. All rights reserved. All product and company names herein may be trademarks of their respective owners.
The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.
If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.