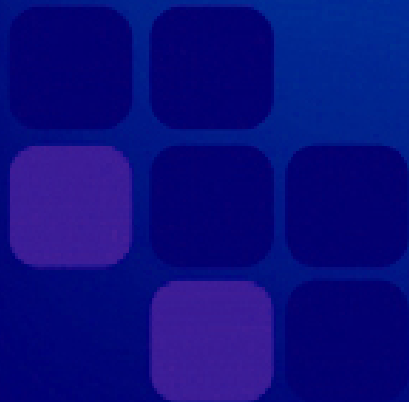


# Secure Online Document Backups:

How Small to Mid-Size Businesses can Centralize Paper and Digital Document Storage Without Sacrificing Security

ClaimProof ™

In this white paper, you will learn how secure and remote online document backups will protect your important business documents and files, whether from being misplaced or lost to anything from theft to natural disasters. Increase productivity and security by keeping remote backups of existing digital and paper files all in one place.



## The Case for Centralizing Business Document Backups

Information is the lifeblood of any business, from customer data to financial records. Mid-sized firms and large businesses often store that information in many places and in many forms.

Some types of document backups are more susceptible to loss or damage than others. Files stored on a single computer can be lost due to a hard drive crash. Paper files can be destroyed in fires, floods, and other natural disasters. Both are vulnerable to theft.

Most businesses today have both paper and digital files, but no storage solution that equally and securely protects all of their important documents. Not only is some business data difficult or impossible to replace, but its loss can have serious financial or reputation-oriented repercussions, such as compromising private customer information.

### Trends in Data Security: Understanding the Risks

The threats to important business data are all too real. From employee theft to the massive storms and flooding witnessed during the last few years, secure document backups are more important than ever.

In fact:

- There were 116,500 non-residential fires in the U.S. in 2007, with direct damages equaling more than \$3 billion.<sup>1</sup>
- From 2004 through 2008, there were nearly 2300 natural disasters worldwide with a Red Cross / Red Crescent emergency response.<sup>2</sup>
- 35% of data breaches occur with lost or stolen laptops and devices.<sup>3</sup>
- When factoring in the average direct, indirect, and opportunity costs associated with a breach of data, the per-incident costs for a company are \$182 for each record breached (which averages to \$4.8 million per company).<sup>3</sup>

Document loss and theft have real repercussions and a real cost. Can *your* company afford the risk? How far will traditional document security practices go to protect your company's most valued data?

---

## Traditional Document Security Solutions

Business executives and security professionals have long understood that data and document loss can cost businesses both directly and indirectly, such as in decreased employee productivity. Because of this, many basic document security features are commonplace, including:

- Encryption and password protection of on-site computers, terminals, and servers.
  - Physical locks on file room doors, office doors, filing cabinets and drawers.
  - Security personnel.
  - Off-site physical backups of paper documents.
  - Disks and remote backups of digital files.
- 

## Additional Document Storage Challenges

Unfortunately, traditional document security solutions don't allow for easy centralization of paper and digital files. The risk of important business documents being lost, stolen, or destroyed isn't the only problem stemming from a non-centralized document backup system. Companies also face the following challenges when using non-centralized document storage strategies:

- **Decreased Employee Productivity** - Employees can't always find everything they need quickly when they have to search a combination of digital and paper files. This can have a direct impact

not only on earnings but on customer service.

- **Difficulty in Controlling Access** - Companies can't always fully control which staff members have access to which files (such as using a main file storage room for all departments or not properly securing physical filing cabinets or systems).
- **Increased Waste** - With many businesses trying to decrease their impact on the environment, both to make a difference and appeal to more eco-conscious customers, having off-site copies of paper files can hurt those efforts with double the amount of paper used.
- **Higher Costs** - Backing up paper documents off-site and creating on-site digital backups both have significant costs involved. Those costs may include storage facility leasing, additional filing cabinets, additional servers, security systems or personnel at those backup storage locations, increased expenses of paper and folders, and higher costs associated with staff time of building and maintaining those backups.

Companies can overcome these challenges by centralizing document backups, where digital and paper files are equally accessible and secure.

---

## **Solution: Secure & Remote Online Document Backups**

Remote and secure online document backups allow businesses to take advantage of centralized file storage, while minimizing many of the burdens previously discussed.

### **Understanding Remote Online Document Backups**

What exactly are remote online document backups, and how do they alleviate document storage concerns?

In their most basic form, "remote" backups simply refer to document and file backups being stored off-site. The storage facility might be managed by the company itself, or a third party document security company may be utilized.



Technically, remote file storage can be in either digital or print form. In an ideal situation, businesses would be able to consolidate all existing paper and digital files into one centralized document storage system. A digital remote storage system generally provides added benefits.

## Benefits of Secure & Remote Online Document Backups

Secure online document backups address many of the storage concerns businesses face. They can offer added security and easier access control for example, while decreasing business costs in maintaining those file backups.

Full benefits of secure and remote online document backups include:

- **Protection From Natural Disasters, Theft, and Loss** - Paper files can be lost or misfiled. Online document backups can be searched for with a simple query, making even misplaced files easy to find. The remote, off-site storage means that even if a natural disaster strikes the company headquarters, or if there is a break-in involving data theft (such as stolen laptops), secure backups of all documents will still be available and easily accessed elsewhere. Companies in disaster-prone areas would benefit from remote document storage solutions with servers located elsewhere in the country.
- **Centralized Paper and Digital Document Storage** - Technology now simplifies the process of creating digital backups of not only existing digital files but *also print documents*. More importantly, businesses don't need a scanner or special document editing software to do so. Access to a standard fax machine is all they need to easily centralize secure document backups.
- **Easier (and More Controlled) File Access** - When documents are securely and remotely stored online through a third party service, employees and executives can access important business documents

 35% of data breaches occur due to lost or stolen laptops and similar devices.<sup>3</sup> 

from anywhere in the world with an Internet connection, 24 hours a day, 7 days a week. Even while on a business trip, employees can access necessary files and documents without having to wait on emails and faxes. The company can also choose to setup group permissions with online services, allowing only specified personnel or departments to access, open, and store specific files or data groups.

- **Lower Document Storage Costs** - By outsourcing secure document backups to a remote online backup service, companies can decrease their own costs. They won't have to spend money on a separate physical storage location, added staff to manage the servers (systems which hold the digital file backups), or storage supplies.
- **Increased Employee Productivity** - When staff can conduct a simple online search of the company's private document storage, they save time and increase productivity over manually hunting for files in filing cabinets. With the ability to limit document backup access to only relevant departments or employees, staff members save further time by not having to dig through unrelated files to find what they need.
- **Increased Document Security** - Paper files can't be secured as well as digital files (locks can be broken and keys can be stolen). Digital backups offer added security with the ability to control file access, encrypt data as it is being stored or downloaded for use, and survive even hardware failure with cloud computing technology.
- **An Eco-Friendly Option** - By eliminating unnecessary paper document backups, companies can decrease their impact on the environment. Not only will they cut down on their paper usage, but they eliminate the transportation emissions of shipping large quantities of paper, reduce electricity needs associated with extra storage facilities, and decrease their reliance on non-environmentally-friendly printer and copier toners.

The benefits of remote document backups and storage are obvious, but some executives and business owners simply feel more secure with physical backups.

Today's technology, however, makes remote online document security something they can rely on.

## How Document Security Works With Remote Backups

Remote document storage services offer a wide range of security features to protect their customer's private data from anything from technical failures to unauthorized access. Those security measures may include:

 A single incident of data breach costs companies \$4.8 million on average.<sup>3</sup>

Can *your* company afford it? 

- **User Access Control** - The primary account holder with the remote document backup service should be able to grant access to multiple employees or departments, while controlling who is able to access any specific file or folder. Users can choose secure passwords to protect documents from unauthorized access on their accounts, while the primary account holder retains the ability to add and remove users (ensuring past employees no longer have access to confidential company data stored there).
- **Cloud Computing Technology** - Cloud computing ensures that a single hardware failure can't destroy documents and backups as failure of a single on-site company server may. It works by storing data on multiple servers, so backups remain even with complete hardware failure of any individual device.
- **Data Encryption** - Data should be encrypted when in transit between the company's hardware (computers) and the remote document backup service. This means that the data is scrambled, sent, and then de-scrambled for storage in a way that prevents it from being recognizable if it should be intercepted in transit in any way. Data can also remain encrypted on-site until the user is ready to download it for use. Information should be made available by any remote document storage service with details on their SSL (secure socket layer) certificate which handles on-site encryption.
- **Secure Repositories** - Because document storage companies understand the importance of data security well, they also understand how to create or use secure physical repositories,

keeping their servers protected not only from natural disasters and environmental issues (such as high temperatures and moisture) but also from unauthorized access of any kind.

- **Third Party Verification** - Third party organizations exist to evaluate Web privacy standards. They will assess privacy and security issues of online services dealing with the transmission and storage of private or personal data. If the service meets acceptable standards of security, they often issue a seal or badge which is displayed on the service's own site as an assurance to customers. TRUSTe® is one of the most trusted third party verification services evaluating remote storage solutions and more, offering increased peace of mind.

Online remote document storage services offer more in the way of protection than many mid-sized companies can implement with their existing staff and storage facilities or equipment. The key is to find secure document backup solutions offering the right combination of security measures and features.

## Five Things to Look for in a Document Backup Service

When choosing a remote secure document backup service for a company's important business documents, several things should be considered:

- **Centralized Document Storage Capabilities** - Many remote document storage services only support the storage and backup of existing digital files. In order to centralize paper and digital document storage, the user would have to scan paper files to a computer and then use software to save it as a scanned image or other file type before backing it up. Instead, look for services that support simple fax backup options to save time. Remember that a benefit of centralized document storage is to increase employee productivity - that won't happen if they're spending unnecessary time converting paper documents to digital files manually.
- **Location** - Because one of the biggest threats to physical document backups is a natural disaster (storms, wind, flooding, or fire), a remote document backup service should have their servers stored in

a secure repository in an area of the country not known to be prone to those types of disasters. This ensures continual access to important business documents, even if disaster strikes a company's physical location.

- **Encryption Capabilities** - No remote document storage service is secure without the ability to encrypt data. This isn't an option to look for - it's a requirement when interested in data security.
- **User Access Control** - Some document backup services only offer a single set of user login credentials (username and password). This may be fine for personal use, but not when securing business document backups. To take advantage of the best security options available, look for services which allow multi-user access (so the master account password never has to be shared). Ideally, the primary account holder should be able to grant different usage permissions to each user under them (or even be able to grant user management permissions to department heads who can then control individual employees' access to data).
- **Multiple Service Level Options** - With one of the benefits of remote online document backups being cost savings, there is no need to spend money on unneeded resources. Solo entrepreneurs will have very different needs than a mid-sized corporation with multiple staff members, and any company specializing in secure remote document backups for important business documents should be capable of equally meeting their needs.

## ClaimProof: Your Documents Simply Secured

Protect your company's important documents and files from being lost, stolen, or destroyed with your ClaimProof remote backup services. We offer you and your employees peace of mind with the ability to backup files *and* paper documents. ClaimProof vaults make secure document backups as easy as 1-2-3. You can upload files directly from your computer, email them for backup, or use our unique fax upload option to digitally save and secure your important paper documents.

### How ClaimProof Protects Your Business Documents

Your company's document backups are available 24 hours a day, 7 days a week from anywhere in the world with an Internet connection from your secure ClaimProof vault.

Those backups protect your business if the originals are lost or stolen, and even increase office productivity by replacing outdated and complicated filing systems.

 ClaimProof is a Certified licensee of The TRUSTe® Privacy Seal Program.<sup>4</sup> 

ClaimProof vaults are completely secure with servers in a secure repository, data encryption in transit and on-site, and user access control for business customers (*you* decide who can access your company's ClaimProof vault and who can access specific files and folders within it).

Documents stored in a ClaimProof vault also benefit from the added protection of cloud computing technology, so you never have to worry about server failure again. Your documents are stored across a "cloud" of servers, networked so others step in to serve your files if another one fails for any reason.

## Highlights for Business and Corporate Users

Several ClaimProof vault options are available for business users, whether a small business or a larger enterprise.

Service Level	Users	Files	Monthly Fax Pages	Pay Monthly	Pay Annually
30 Day FREE Trial	1	25	5	FREE	n/a
Business Plan 1500	3	1,500	30	\$29.95	\$299.50
Business Plan 3000	4	3,000	50	\$49.95	\$499.50
Business Plan 6000	5	6,000	80	\$79.95	\$799.50
Enterprise Plan 12000	7	12,000	120	\$119.95	\$1,199.50
Enterprise Plan 24000	10	24,000	200	\$199.95	\$1,999.50
Enterprise Plan 48000	20	48,000	300	\$299.95	\$2,999.50
Additional Users	1	n/a	n/a	\$9.95	n/a

[Sign up for a 30 day free trial today](#), and discover for yourself how a ClaimProof vault will centralize your digital and paper file storage, protect your important business documents from theft and natural disasters, positively impact your office productivity, help your company cut down on paper waste, and offer greater security and control over who can access confidential company data.

---

<sup>1</sup> U.S. Fire Administration. (2008, September 19). USFA Non-Residential Fire Statistics. Retrieved March 18, 2009, from <http://www.usfa.dhs.gov/statistics/national/non-residential.shtm>

<sup>2</sup> International Federation of the Red Cross and Red Crescent Societies (IFRC). Disaster-Related Statistics. Retrieved March 18, 2009 from <http://www.ifrc.org/what/disasters/resources/statistics/2004-2008.asp>

<sup>3</sup> Ponemon Institute, LLC. 2006 Annual Study: Cost of a Data Breach, Understanding Financial Impact, Customer Turnover, and Preventative Solutions. Retrieved April 12, 2009, from [http://www.computerworld.com/pdfs/PGP\\_Annual\\_Study\\_PDF.pdf](http://www.computerworld.com/pdfs/PGP_Annual_Study_PDF.pdf)

<sup>4</sup> TRUSTe. ClaimProof Validated Privacy Statement. Retrieved April 13, 2009, from <http://www.truste.org/ivalidate.php?url=www.claimproof.com&sealid=101>