A Guide to Proper Data and Document Destruction

Shred Nations | @ShredNations

Table of Contents

Introduction

It seems as though news headlines shine the spotlight on new examples of data breaches caused by improper in-house document shredding and disposal. While the average passerby may not think of these companies as being anything more than in the wrong place at the wrong time, savvy business owners should take this as an opportunity to learn from the faults of other companies.

As other major businesses have unhappily demonstrated in recent years, there is newfound importance on proper document and media destruction, and although shredding your documents in-house and as part of your day-to-day tasks can seem logically more simple and less expensive, this option carries quite a bit of risk.

So the question now becomes for businesses hoping to protect their employees, customers, and credibility, what *is* the proper way to shred and dispose of your no-longer-necessary documents and records?

Over the past five years alone digital technology has continued to rapidly advance, bringing confusion hand-in-hand with all the convenience of new and improved tools. Although there have been plenty of new ways of managing your information, as business owners this now means there are also new ways of properly shredding and disposing of documents as well.

Not only will this article help to identify examples of improper document destruction policies, Shred Nations also strives to outline what media and information poses the greatest risks to businesses for data breaches as well.

After isolating any potential gaps in your company's information security, we can also help you with developing the best strategies and practices for ensuring that all company documents are safely and securely shredded and disposed of through Shred Nation's mobile shredding, off site shredding, and drop off shredding services.

Examples of Improper Document Destruction

Given the long-lasting impacts of a data breach, improper destruction and disposal of business data or documents has become a cardinal sin in the modern world of business—a lesson that many companies have unfortunately had to learn the hard way.

Taking the case of New York-based healthcare company Affinity Health Plan as an example—where a [$1.2 million payment was agreed upon in 2013](#) to settle an information privacy case—there is little forgiveness for businesses that take data and document destruction lightly.

According to the case, the leased photocopier had been a part of an investigative story by CBS evening news. With three other unknowing participant businesses like Affinity Health also included, the company that had previously leased the copiers had then sold the machines to CBS, who hired a separate firm to later analyze the hard drives of the returned photocopiers.

Unfortunately for Affinity, company data was discovered by CBS when [confidential patient health records](#) were found to still exist on the hard drives of Affinity Health's photocopy machines, opening the floodgates for criticism in the public eye as Affinity took center-stage on the nightly news.

While the hefty $1.2 million fine may seem like punishment enough, this really only scratches the tip of the iceberg in terms of the potential impact of improperly destroying and disposing of company documents.

Between PR-crippling news stories of your company security gaps and the mere cost of having to recover and reorganize all your compromised company information, the implications of not handling your data and documents correctly should be more than enough to leave you doing your best to toe the line.

Common Document Storage Methods

Besides traditional paper documents that have long-dominated the world of business records and information, advances in office technologies over the past half-century have also opened a new Pandora's box of documents and data to manage for your business. While some may not realize it, when technologies like a photocopy machine allow a document to be reproduced, an internal copy of the document is also made by the machine, which—as in the case of Affinity Health—cannot be discounted when it comes to properly destroying and disposing your business records.

Virtually every office machine you will encounter has a method of storing the data that it faxes, scans, or sends—including even the $20 home printers you can buy at Office Depot. Sensitive information often tends to surround you in your office, and by simply keeping yourself aware and up-to-date on where to find it, you can stay one step-ahead of those potentially trying to steal your valuable company data and documents.

To give you a better idea of the different storage vulnerabilities that may be putting your business data at risk, here are a few of the most common document storage devices seen around the office today, and some of the safest ways to dispose of the valuable information they store:

Photocopiers

Before modern digital technologies became mainstream in an office, older photocopiers used xerography to reproduce images—often times referred to as "xeroxing"—which did not need to create an internal copy of an image to reproduce a paper version. Today however, as Affinity Health Plan unfortunately demonstrated for other potentially unknowing business owners, frequently used digital photocopiers pose a much greater potential risk to the security of your consumer and company documents.

Although several office devices that are connected to your company network are now more likely to include security features that directly address possible gaps in information security, human error continues to be a top contributor to data breaches. To get a better handle on keeping data disasters like Affinity Health's at bay, one of the best things your business can do to protect itself is plan for the worst.

By keeping your employees informed on potential vulnerabilities like a copy machine's internal hard drive, you can make a good start, but many data security experts will also suggest that you implement a periodic plan to wipe old data from your company machines. That way, you can already begin to nip a potential

problem in the bud by simply limiting what both employees and data thieves alike have access to.

Fax Machines

Much like the digital photocopiers used today, modern fax machines generally now store digitized information as records of the faxes that are sent on the device. As with other digital technology and documentation, this data stored to the machine hard drive is much more easily accessible than the hard-copy information of yesteryear, although that doesn't put older thermal fax machines entirely out of harm's way yet either.

While modern fax machines take the information you are faxing and save a copy of the document to the machine's internal hard drive, traditional thermal fax machines took the original document and copied the image to a roll of thermal film in order for the fax machine to then transmit to the recipient.

When modern fax machines began to take the place of thermal faxing, many businesses dumped or donated their old machines without removing the film, leaving anyone with a sense of curiosity open to easily access whatever information was left inside.

Today common data disposal practices for fax machines include first ensuring that old film from thermal fax machines is securely shredded and destroyed before disposing or upgrading to digital models, in addition to setting up a regular document disposal plan for all your digital and hard-copy company data.

Hard Drives and Old Computers

When it comes to digital technologies, business information is constantly being stored on various devices, and often times documents are so small and there are so many that they can overwhelm your business. Between the current computers in your office, any thumb drives you may be using, or optical media stored on CDs and DVDs, there are a multitude of sources for your current company data—not to mention what may lay dormant on old devices.
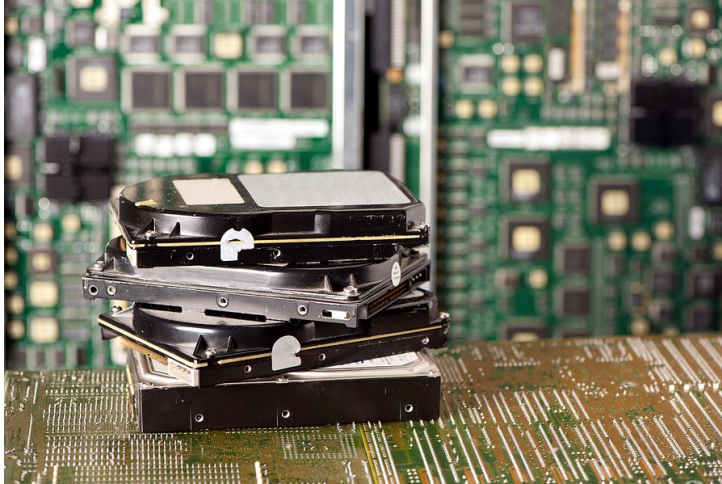
For newer digital devices, a software solution may be your best option, as overwriting or "wiping" your storage device will allow you to safely dispose of any sensitive information the device still contains. This way, if your business plans on re-selling or returning a leased device, your company information can be securely disposed of and protected without rendering the device useless for future use.

Legacy media forms like floppy drives or zip disks can also be found occasionally lying around, as well as old computers and hard drives you may be readying to retire from your business—but before doing so, be sure to cover all your bases by properly destroying any old information or data that could be still left on them.

Whereas newer technologies and devices tend to hold value for their reusability—making less-permanent software solutions to wipe a computer hard drive more appealing—old media and document storage devices are usually just donated or thrown out. As a result, most experts advise business owners to instead opt for mechanical destruction of hard drives and other similar storage devices.

Comparable to paper shredding for machines, physical hard drive destruction essentially fills the same purpose of ensuring that your documents can never be recovered by a potential data thief. While there are a few specific ways that a hard drive can be physically destroyed—from degaussing to hard drive shredding and crushing—the end result is the same: the hard drive cannot be accessed again after its destruction.

Though there are certainly pros and cons to either method of document [destruction and disposal for hard drives and electronic media](#), it can be hard to say for certain if one is more secure than the other. If you truly want absolute assurance of your business information and data being securely disposed of, you should have your devices additionally wiped before they're manually destroyed to guarantee you've utilized every safeguard available.

Traditional Paper Documents

In today's world of business digital documents have started to become more the norm, but there are still plenty of companies that have traditional hard-copy documents around the office. The reasons for keeping paper records can range widely—from mandated document retention laws like HIPAA, to simply not getting around to a document scanning project and making the transition from paper to digital.

Depending on the scale and type of business, proper document destruction and disposal policies can also vary. For the most part, many information security experts advise the adoption of a shred-all policy for your company, as it tends to be something of a catchall and usually one of the safer options out there.

If you are the owner of a financial firm or business that handles sensitive employee or consumer records, a less-general alternative to shred-all policies may be a better option—you can still adhere to document retention laws without putting yourself at risk for a potential data breach. For documents like bank statements, employee payroll records, and business invoices, there are retention period guidelines that can help you to manage your critical company documents without cluttering your office.

To help minimize the chances of crucial business information falling into the wrong hands, it's highly recommended that business owners remain up-to-date and brushed up on the best practices for destroying and disposing of your business documents—both digital and hard-copy alike. By covering all your bases and ensuring that your valuable company data is safely and securely destroyed, you can save your business from hefty fines and help to avoid your company being just another bad example for others to learn from.

So after now identifying the biggest potential gaps in your wall of information security, the next question becomes how best to address them. Between in-house, offsite, or mobile document shredding and disposal, which will work best for your company?

Destroying Your Business Documents In-House

In the event of a data breach, a company can lose so much more than money, making it a good idea as a business owner to always be aware of the best practices to protect your company. Safeguarding both company and customer data is both a critical and constantly evolving practice that both yourself and your employees should remain up to date on. Although generally speaking, information security experts will advise against trying to manage document shredding and destruction on site, here is a brief overview of the pros and cons of in-house shredding:

Potential Advantages to In-House Document Disposal

To ensure that your business is secure from top to bottom, data and other information security must extend beyond just the IT department. When you adopt an in-house document destruction program, this makes for an excellent opportunity not just to personally oversee the regular destruction and disposal of company documents that could put your business in harm's way, but to also take a moment to teach best data security practices to your employees as well.

Dangers of Destroying Your Business Documents In-House

The risks involved with in-house document destruction stem from the increased likelihood of a data breach occurring. By implementing a company-wide shredding policy, you potentially expose confidential information and data to employees that may not even be intended for their eyes to see.

Furthermore, when employees are asked to take on tasks that are unrelated to their core responsibilities, they may be more prone to make mistakes or simply disregard your policies altogether—which in either case could spell disaster for your company.

Every business has information that they must shred, destroy, or dispose of in one way or another, and no matter the size of the company, ensuring you have the proper document destruction policies in place is a key component to keeping your critical company information safe and secure.

Offsite and Mobile Document Shredding and Disposal

When it comes to managing a company's paper and electronic media documents, storing and shredding them on site tends to be fairly risky. When you take your chances on handling your confidential information in-house, you also take your chances with your company's credibility, customers, and employees.

So with these potentially long-lasting impacts on one hand, what is a truly safe route for shredding or destroying sensitive documents? If this same question has run through your mind, consider services like mobile shredding or off site shredding for your solution.

With mobile shredding, a safe and secure shredding truck actually comes to you to complete your shredding project, conveniently destroying your documents while you watch at your curbside. Our self-contained shred trucks are equipped with industrial shredders capable of destroying over 6,000 pounds of material in an hour, making a single shredding project a mere matter of minutes.

Similar to mobile shredding services from Shred Nations, our secure off site shredding facilities and services are designed to ensure that your sensitive documents are kept both safe and secure while also being destroyed in compliance with all state and federal laws. A slightly cheaper option when compared to mobile shredding given the convenience of shredding on site, our customers are still given a formal certificate of destruction following off site service as proof of proper shredding.

The following is a short breakdown of the various advantages and disadvantages of both mobile and offsite document shredding:

Pros and Cons of Mobile Shredding Services

No one wants the headache and hassle of gathering up and hauling all your documents down busy highways and streets to be shredded across town at a shredding company. With mobile shredding however, you can have a mobile shred truck come to your home or business location to pick up and shred your documents.

Our trained shredding professionals never come in contact with your documents locked in shredding containers, and will present you with a certificate of destruction after their service is complete, guaranteeing that all document destruction complies with shredding laws like FACTA and HIPAA.

Although mobile shredding services are convenient for businesses needing smaller amounts of documents shredded, this option can become more expensive when a company has large amounts of documents which require regular shredding.

Pros and Cons of Offsite Document Destruction

Offsite shredding services from Shred Nations are similar to our mobile shredding services. We send a shredding truck to your business to collect your locked shred bins and transport them to a safe and secure offsite shredding facility. You are also presented a certificate of destruction to ensure proper disposal of your sensitive information.

One difference from mobile shredding, however, is that offsite shredding tends to be more cost-efficient for companies with large-scale shredding. While mobile shredding services usually charge per trip to your site—generally about $100 for a visit to pick up 15 boxes—off site shredding generally tends to be less expensive since the documents must only be collected during the stop, usually running around $85 for a project of the same size.

While offsite shredding is considered a better value for shredding larger quantities, many documents and other materials can be so sensitive that their destruction must be witnessed. Surprisingly though, witnessed shredding is actually a more common request than one may think, and if you too find yourself in this category, Shred Nations' mobile shredding services are your best bet.

As you can see, when it comes to managing and disposing of both your personal and business documents, there are numerous options to consider and choose from—although some are certainly a safer bet than others. In the case of trying to store and

shred your business records and documents in-house for instance, the odds for miscommunication and eventual disaster are quite high.

With mobile shredding, drop off shredding, or off site shredding services on the other hand, the potential benefits to each strategy stretch onward. Not only does each shredding service act as something of an insurance policy—safeguarding against unintentional noncompliance with state and federal information privacy laws—they can simply make both your life and the life of your employees a more simplified one.

Keeping straightforward catchall rules for how your business decides to keep and manage information can vastly minimize your company risk for a data breach. By just reducing the amount of valuable information you have to protect, your business will in turn have less to lose as well—shrinking any sort of crosshair a data thief may have trained on your company's information.

When you know that all your document management and shredding is being properly managed, you can produce more productive and efficient results in your daily duties without concern for it being entirely undermined by catastrophic data breach.

Conclusion

Depending on the business and its overall size, business owners are faced with several choices for how to manage and dispose of company data and documents without putting their own business at risk for a major data breach.

Although there generally are numerous factors and data storage places to keep in mind, at the end of the day the essential point that must be kept in mind by business owners is what your chief priority is. Some of the most important questions to consider:

- **How Much Material Will You Need Shredded?** Do you know how many documents are in those boxes? If you're looking at a shredding project with more boxes of documents than you can count on two hands, give off site shredding a thought. This way, you can spare your budget at least a little breathing room, while ensuring every document is securely disposed of by our industrial shredding machines.

- **Is Time a Factor?** If you simply just don't have the time to gather your boxes of documents and haul them down to a Shred Nations nearby drop off location or off site shredding facility, then mobile shredding services are your solution. They come to you, shredding your documents at your curb in less than fifteen minutes—letting you get back to your already busy day.

- **Are You a Law-Abiding Citizen?** With numerous information privacy protection laws like FACTA and HIPAA in place and new ones cropping up seemingly each day, ensuring your business has all its legal bases covered when it comes to document shredding can become quite the burden. With Shred Nations offsite and mobile shredding services however, your certificate of destruction ensures these laws are all adhered to, and better yet—if you are even legally required to witness your documents being shredded, you can watch a mobile shred truck destroy your documents right there on the curb!

There are pros and cons to both mobile and off site shredding services from Shred Nations. For small companies which only need shredding done occasionally, a mobile shredding purge may be all that is necessary for the job. The larger the company and the more information needing to be stored and referenced frequently on the other hand, a regularly scheduled weekly, bi-weekly, or monthly off site shredding will become more cost effective without sacrificing the safety and security of sensitive company information.

Get Free, No-Hassle Quotes on Offsite and Mobile Data Storage Options!

To learn more or for further assistance finding the best service option for your company, feel free to contact us—Shred Nations can help to set up business owners with safe, secure, and reliable mobile, offsite, and drop off shredding services in your area. **Just fill out the form to the right, or simply give us a call at (800) 747-3365 today!**

Additional Resources

Protecting Your Company Against Fraud & Theft

In a world full of data breaches, identity theft, and increasingly important online security, it can be easy to lose sight of some of the most obvious gaps for corporate spies to exploit in your defense. Let us help you to identify the different threats to your company's hard-copy and digital documents alike, and figure out the best ways to protect your information from a costly data breach.

Shredding for Business—Retention Times & More

Shred Nations has been providing mobile shredding services and offsite shredding services to corporations and businesses nationwide for decades. Learn about the advantages of hiring a secure shredding service for your business, from business document retention times to detailed information on Electronic Media Destruction and Hard Drive Shredding.

Warning: You're Losing Money Shredding Documents Internally

So you've purchased a shredder. Your secrets are now safe, your sensitive information is secured, and you can't be accused of improperly disposing documents, or worse yet, obstruction of justice—right? Wrong. This article outlines why it is more secure, better business, and a far better legal strategy to use third party experts to certifiably destroy documents.

Shredding Laws, Compliance, and Security

State and federal shredding laws affect each company and industry separately, but play a key role each time you decide how and when to shred your documents. Learn about the different laws in the United States and all the compliance and security measures your company can employ to ensure you avoid a disastrous data breach.