



USING DOCUMENT SHREDDING TO SAFEGUARD AGAINST DATA BREACHES

2017 | JANUARY EDITION

HOW DOCUMENT
SHREDDING PREVENTS
DATA BREACHES



**COPYRIGHT © 2017
SHRED NATIONS**

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of the publisher, except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law

**777 S WADSWORTH BLVD 3-250
LAKEWOOD, CO 80226**

SHREDNATIONS.COM



DATA BREACHES: A GROWING THREAT TO BUSINESS

BY RYAN MCHUGH

Cropping up with increasing frequency in nightly news reports, **data breach incidents** are becoming a more pressing threat to address than ever.

With advancing technology, even the smallest amounts of leaked personal or proprietary information can lead to disasters like data breaches, making it essential for business owners to now plan for and protect against these risks that can lead to millions of dollars in losses, potentially irreversible damage to company reputations, and even cripple small businesses entirely.

Although many businesses may now be wondering what they can do to protect themselves, with this in-depth

white paper we help to answer these questions, providing companies the breakdown on how various **document shredding** strategies can minimize the risks for data breaches while keeping company information secure.

WITH ADVANCING TECHNOLOGY, EVEN THE SMALLEST AMOUNTS OF LEAKED PERSONAL OR PROPRIETARY INFORMATION CAN LEAD TO DISASTERS LIKE DATA BREACHES.

Hackers, identity thieves, and other malicious individuals are constantly finding new ways to penetrate companies' defenses and steal personal or proprietary information, and besides simply sowing chaos within companies, these data breaches often come with significant financial hardships for businesses.

Each year, the cost and impact of data breaches continues to rise—now **crossing the \$4 million threshold** for the average consolidated total cost of a breach as of 2016, with each lost or stolen piece of sensitive information now running an average cost of \$158.

Furthermore, according to **a recent study** nearly 85% of customers refuse to shop or use companies after a data breach, compounding the already significant costs of the breach itself with lost business during a time when the company needs to recover.

With risks for data breaches ranging from accidental misplacement of records to confidential documents being outright stolen, businesses must now ask themselves how they plan to protect against breaches.

This is where paper shredding comes into the picture. Here we take a closer look at how companies are now working to fight back against the threat of data breaches

with the help of shredding, and provide insight into the various ways businesses can use **document shredding** to help safeguard both their sensitive information as well as their business.

EACH YEAR, THE COST AND IMPACT OF DATA BREACHES CONTINUES TO RISE – NOW CROSSING THE \$4 MILLION THRESHOLD FOR THE AVERAGE CONSOLIDATED TOTAL COST OF A BREACH AS OF 2016, WITH EACH LOST OF STOLEN PIECE OF SENSITIVE INFORMATION NOW RUNNING AN AVERAGE COST OF \$158.



HOW DOCUMENT SHREDDING COMBATS DATA BREACHES

While it's important to ensure documents with personal, proprietary, and any other sensitive information are secured and retained for the necessary time, it's critical for companies to also account for disposing and shredding these documents.

Once they no longer need to be kept businesses should securely shred documents, and not just because shredding frees-up storage space and keeps offices organized—document shredding is also an essential part of [data breach prevention plans](#).

With potentially irreversible damages to public reputations and the chances for steep fines for noncompliance with [data destruction and retention laws](#), data breaches both directly and indirectly cost companies millions each year.

Although there are dozens of ways for malicious individuals to steal information from businesses and individuals, this doesn't mean there aren't ways of protecting oneself. By shredding sensitive information, the amount of sensitive information to potentially abuse is kept to an absolute minimum—in turn helping to minimize the chances for stolen documents and records to lead to data breaches.

Despite this protection however, it's important to not lose sight of the fact that paper shredding can only provide protection to the extent of how often and what you shred.

Over the course of a year, businesses accumulate a fair amount of sensitive information, and like cleaning the dirt from a car, it's generally a good idea to clean it more than once a year. Even if you plan to eventually shred them, they are as vulnerable to theft while waiting for shredding as they are sitting in an ordinary dumpster.

With this in mind, it's important to establish a sound [document management and destruction plan](#). Using document management helps businesses to develop optimized workflows that give appropriate consideration to document security and shredding.

By implementing retention and destruction schedules, documents can be maintained and destroyed according to retention guidelines before being regularly shredded—helping to not only eliminate the risk of old documents leading to legal issues, but also cutting down on the associated costs of storing them.

Shredding is a crucial component to document security, and one of the first and easiest steps companies can take to ensure they avoid disasters like data breaches. There are a range of strategies and programs companies can integrate, and so while shredding leaves businesses the opportunity to find the processes that suit them, all roads end with high priority on [proper document disposal](#).

ALTHOUGH THERE ARE DOZENS OF WAYS FOR MALICIOUS INDIVIDUALS TO STEAL INFORMATION FROM BUSINESSES AND INDIVIDUALS, THIS DOESN'T MEAN THERE AREN'T WAYS OF PROTECTING ONESELF. BY SHREDDING SENSITIVE INFORMATION, THE AMOUNT OF SENSITIVE INFORMATION TO POTENTIALLY ABUSE IS KEPT TO AN ABSOLUTE MINIMUM—IN TURN HELPING TO MINIMIZE THE CHANCES FOR STOLEN DOCUMENTS AND RECORDS TO LEAD TO DATA BREACHES.



USING SHREDDING TO STOP DATA BREACHES

While implementing a shredding policy where complete document inventories are taken and certain documents are destroyed according to retention schedules is an extremely effective way of managing information and document security, some of the questions to first answer are what will be destroyed, how it will be destroyed, and who will do the destroying.

There are several different options and strategies companies have for protecting personal and proprietary information from a low-tech data breach where hard-copy documents are compromised.

Ranging from integrating new shredding policies and **shredding methods**, to taking a second look at document and information management processes, here are a few of the top ways shredding can be used as a powerful tool against data breaches:

SHRED-ALL POLICIES

A sweeping shredding policy designed to shred anything and everything, **shred-all policies** work exactly as their name implies. Once documents of any kind are no longer needed or useful, they're shredded, working to eliminate any question of what information poses risks worth shredding.

One of the greatest advantages to adopting a shred-all plan, having zero documents for a thief to steal leaves little room for data breaches. While many breaches stem from mistakes about what documents need to be kept and where, shred-all policies simplify the question—removing the decision-making and instead ensuring you err on the side of caution.

Additionally, shred-all policies cut out the cost and time for employee data destruction training and help to free up time for more efficient uses. Rather than holding new training sessions each time policies are updated, a “once you're done with it, shred it,” policy is easy to teach and enforce.

Whether it's a mobile shred truck coming to the office or an off site shredding facility, all it takes is for documents

A SWEEPING SHREDDING POLICY DESIGNED TO SHRED ANYTHING AND EVERYTHING, SHRED-ALL POLICIES WORK EXACTLY AS THEIR NAME IMPLIES. ONCE DOCUMENTS OF ANY KIND ARE NO LONGER NEEDED OR USEFUL, THEY'RE SHREDDED, WORKING TO ELIMINATE ANY QUESTION OF WHAT INFORMATION POSES RISKS WORTH SHREDDING.

to be placed in **secure shredding bins** after they're used to ensure the sensitive information they contain is protected.

The only caveat to shred-all policies is when businesses frequently deal with documents that require extensive retention periods.

Since document storage and retention is **regulated by complex laws and standards pertaining to industries**, in many cases shred-all policies can be less ideal because they don't account for document retention, however, there are other opportunities available to create shredding policies that do account for these needs.

UPDATES TO INFORMATION AND DOCUMENT MANAGEMENT PROCESSES

When businesses need to put as much emphasis on legal compliance and document retention as they do for secure document disposal, all-encompassing policies like a shred-all program are often too general to meet these needs.



To account for all necessary document destruction and retention requirements, it's important to create a thorough **document management plan** which addresses the entire lifecycle of documents from their creation to their eventual destruction.

First and foremost, document management plans begin with conducting a complete inventory of company documents. By evaluating all records needing storage and destruction, businesses are able to implement the necessary **records retention programs** and destruction processes to maintain and optimize their workflow.

With a clear idea of the information needing protection, proper retention guidelines can be established with regular destruction schedules so that old documents aren't kept around to lead to eventual legal troubles, while still-needed documents can still be safely stored.

While documents are being retained, businesses usually prefer to manage their hard-copy documents using secure **off site records storage** locations. Much like how shredding at the end of retention periods ensures there's no opportunity for a data breach post-disposal, off site storage facilities provide another option for protecting sensitive company information that's still needed.

By utilizing off site storage, documents are kept in locked, climate-controlled storage rooms where they have a heightened level of protection compared to ordinary filing cabinets in an office corner.

Adopting and implementing a document management plan can be an excellent alternative to a shred-all policy—they're able to ensure company compliance with all applicable laws and help keep track of documents throughout their retention, but without sacrificing the security programs like a shred-all policy can provide.

SHREDDING SERVICES

Integrating a company shredding policy is an effective way to manage a company's potential exposures to data breaches and ensure information is properly disposed.

Whether it's by a shred-all policy, or through regularly scheduled shredding in a document retention and destruction process, companies have several options for shredding their documents which each come with their respective advantages.

Below we highlight some of the best options and methods businesses have for securely shredding and disposing of sensitive information:

MOBILE SHREDDING

Mobile shredding is not only one of the most convenient shredding options available to businesses, it's also one of the most secure.

Much like the name implies, with **mobile shredding** a truck mounted with an industrial shredder comes to directly to homes or business, shredding the documents on site while clients watch.

Before shredding, businesses store their documents for destruction in **locked shredding bins** supplied by the mobile shredding provider. When documents are actually shredded, they're lifted in the shredding bins using mechanical arms—much like a garbage truck—to dump the documents into the truck's onboard shredder.

As a result, businesses are not only assured that no one besides themselves comes in contact with documents before they're shredded, but they also get to witness the process to provide an extra sense of security throughout the destruction process.

Offering a formal **certificate of destruction** to detail the shredding and ensure compliance with destruction laws, mobile shredding services are often the go-to option for businesses, as they not only help to improve security and keep sensitive information from being misused, but are also by far one of the most convenient ways to shred documents.

OFF SITE SHREDDING FACILITIES

Geared toward companies with shredding needs on a larger-scale than most, off site shredding offers many of the same security benefits and data breach protections as mobile shredding.

Varying slightly from mobile shredding in terms of process, the main difference between the two is where the documents are shredded. As its name suggests, with an **off site shredding service** documents are picked up and transported to a secure facility before they're shredded, rather than the documents being shredded from the curbside.

Having documents picked up and transported instead of shredded on site offers businesses a budget-friendly benefit compared to on site shredding, as off site shredding entirely eliminates the costs of mobile shredding trucks making the trip and staying at the location, rather than making a quick pick up.

While off site shredding does remove the ability to witness shredding—which for some businesses can be a requirement for shredding policies—this doesn't mean off site shredding services offer any less security and data breach protection than mobile shredding.

Incorporating security inclusions of mobile shredding such as secure shredding bins, off site shredding providers also provide certificates of destruction to assure businesses that all shredding is conducted in compliance with destruction laws like **FACTA** and **HIPAA**, and to additionally provide proof of when and where the shredding was done.





CONSIDERATIONS TO KEEP IN MIND

There are a range of threats for data breaches, as well as a range of services and strategies businesses can employ to protect from data breaches.

Whether using **mobile or off site** to specifically shred specific documents according to retention schedules or for a wide-sweeping shred-all policy, document shredding in all forms provides businesses secure, reliable, and efficient protection from disasters like data breaches and identity theft.

So as you now consider or re-evaluate your own policies and processes for implementing shredding policies and securing sensitive information, be sure to keep these final considerations in mind:

HOW OFTEN DO YOU NEED SHREDDING?

If your business finds itself scheduling with a mobile shredding provider too often and costs are running high, this could be a sign you need services to accommodate shredding on slightly larger scale. By opting for off site shredding instead, businesses can find the perfect solution to this problem and keep document security affordable.

WHERE DOES RETENTION COME INTO PLAY?

If your company doesn't deal in documents with extensive retention times, shred-all policies provide one of the most surefire ways of ensuring that sensitive information is protected from misuse or misplacement. If on the other hand retention is a high priority, it's essential your business takes the time to develop a document management plan to account for safe storage during retention as well as secure shredding once it's time for disposal.

ADDITIONAL RESOURCES

Case Study: Why Paper Documents Pose as Much Risk for Data Breaches as Digital

Despite new threats for digital data breaches, security experts still stress that companies not forget traditional paper risks as well. For those who aren't convinced yet, this case study takes a look at a prime example of a company that learned this lesson the hard way in order to help give a better idea of the hard-copy threats to be on the constant lookout for—and how to protect from them.

Protecting Your Company Against Fraud & Theft

When news stories of computer hacking and digital data breaches cropping up seemingly each day, it can be easy to lose sight of other, hard-copy risks for theft and fraud threatening your company. With this in-depth white paper we take a closer look at how paper documents factor into information security today, and why having a well-established document destruction plan can help bolster your defenses.

Safeguard Your Identity

Over the past few years, the already-staggering number of identity theft cases has steadily risen. Compounded by the new potential using electronics for a single piece of stolen personally identifiable information to lead to long-term damage, learn more about how to keep vulnerable information protected from identity theft risks both new and old here.