Protecting Your Documents Against Fraud &Theft

Shred Nations | @ShredNations

EXECUTIVE SUMMARY

In the digital world full of data breaches, computer hackers, and online security, we sometimes lose focus of some of the easiest ways that corporate spies and identity thieves can get information.

Hard-copy documents are something that are used in a lot more companies than you think- and if you don't protect them, you run the risk of losing more than just a few pieces of paper.

With government and other agency requirements to hold on to hard-copy records for years, you need to have a secure, reliable way to manage them from the day they were created to the day they are destroyed.

That's where this article can help you! Learn more about the different threats to your company's hard-copy documents, and let us help you figure out the best ways to protect your company from a costly data breach that can cost you your reputation and millions of dollars.

TABLE OF CONTENTS

INTRODUCTION

The threat of corporate espionage, identity theft, and fraud is real. Sure, it has always been there- there are examples of all three throughout the history of the United States- dating back to the 1800's. The impact is quite impressive:

- *For corporate espionage, U.S. Senators Orrin Hatch (R-Utah) and Chris Coons (D-Del.), who introduced the Defend Trade Secrets Act in April to give trade secrets the same legal protections as other forms of intellectual property, estimate the financial loss due to corporate espionage are between* ***$160 billion and $480 billion each year****.*

- *Approximately 16.6 million people experienced at least one identity theft incident in 2012 (the most recent data available) and financial losses* ***totaled $24.7 billion****. That's an average loss of around* ***$1,500 per victim****. The overall cost of identity theft to the American Economy is estimated to reach* ***$100 billion annually****.*

- *According to the data, annual fraud costs reached* ***$32 billion in 2014****, a 38 percent increase over 2013, which has galvanized calls for more secure payments processing from both private companies and public officials.*

That's hundreds of billions of dollars of losses, and that number is increasing exponentially every year. How do you protect against threats that could ruin your reputation, kill your business, and cost you millions of dollars in the process?

Here is some insight into what corporate espionage, identity theft, and fraud look like, and some things you can do to safeguard your business, minimize the risks of a data breach, and optimize and streamline your processes.

Corporate espionage

Corporate espionage can have a tremendous impact on any business. The main purpose of any kind of espionage is to gather knowledge about organization(s).

It can involve any aspect of a business, from sales to marketing to research and development.

Here are just a few examples that could be at risk if you're the victim of corporate espionage:
The acquisition of Intellectual Property, including:

- Intellectual property
- Industrial manufacturing
- Ideas, techniques and processes
- Recipes and formulas

Requisitioning of proprietary or operational information, including:

- Customer datasets
- Pricing
- Sales/marketing
- Research and development
- Policies
- Prospective bids
- Planning or marketing strategies
- Changing compositions/location of production

Corporate Espionage can even describe activities such as theft of trade secrets, bribery blackmail, and technological surveillance.

Identity Theft

Identity theft is the ever-growing threat for individuals and businesses. It just takes one data breach to expose thousands of customers to unsavory folks that use their personal information against them.

Simply put, Identity theft is a form of stealing someone's identity where someone pretends to be someone else by assuming that person's identity to gain access to resources or obtain credit and other benefits in that person's name.

Identity thieves are trying to obtain anything that can be used on its own or with other information to identify, contact, or locate a single person, or to identify an individual in context.

Government and most companies identify these items as Personally Identifiable Information, or PII, which are the main objectives of identity thieves worldwide:

- Full name (if it's not a common name i.e. John Smith)
- Home address
- Email address (if it's a private email address from an association, club, membership, etc.)
- National identification number

- Vehicle registration plate number
- Driver's license number
- Face, fingerprints, or handwriting
- Credit card numbers
- Digital identity
- Date of birth
- Birthplace
- Genetic information
- Telephone number
- Login name, screen name, nickname, or handle

Fraud

Fraud is officially defined as an act or course of deception, an intentional concealment, omission, or perversion of truth, to gain unlawful or unfair advantage, induce another to part with some valuable item or surrender a legal right, or inflict injury in some manner.

Just to be clear, incompetence or negligence in managing a business or even a reckless waste of firm's assets (by speculating on the stock market, for example) does not normally constitute fraud.

Here are some of the most common types of fraud:

Telemarketing Fraud

When you send money to people you do not know personally or give personal or financial information to unknown callers, you increase your chances of becoming a victim of telemarketing fraud.

Nigerian Letter or "419" Fraud

Nigerian letter frauds combine the threat of impersonation fraud with a variation of an advance fee scheme in which a letter mailed from Nigeria offers the recipient the "opportunity" to share in a percentage of millions of dollars that the author—a self-proclaimed government official—is trying to transfer illegally out of Nigeria.

Letter of Credit Fraud

Legitimate letters of credit are never sold or offered as investments. They are issued by banks to ensure payment for goods shipped in connection with international trade. Payment on a letter of credit generally requires that the paying bank receive

documentation certifying that the goods ordered have been shipped and are en route to their intended destination.

'Ponzi' Schemes

"Ponzi" schemes promise high financial returns or dividends not available through traditional investments. Instead of investing the funds of victims, however, the con artist pays "dividends" to initial investors using the funds of subsequent investors. The scheme generally falls apart when the operator flees with all of the proceeds or when a sufficient number of new investors cannot be found to allow the continued payment of "dividends."

Pyramid Schemes

Pyramid schemes—also referred to as franchise fraud or chain referral schemes—are marketing and investment frauds in which an individual is offered a distributorship or franchise to market a particular product. The real profit is earned, not by the sale of the product, but by the sale of new distributorships.

As you can see, there are dozens of ways mentioned (and hundreds that weren't) that corporate spies, identity thieves, and shady businessmen can use to appropriate information, corporate secrets, and money from individuals and businesses.

No company is immune- if your company is profitable, or has a great idea, there's a chance that someone will try to take it from you. The best way to protect yourself is to have a plan of attack to protect your business and ensure that your information is secure.

Data breaches cost companies billions of dollars every year- and that number is increasing! Our goal is to give you some sound advice to help minimize the risk of hard copy files, documents, and records compromising your business.

Protecting your company from Corporate Espionage, Identity Thieves, and Fraud

Create a Sound Document Management Plan

Document management includes methods and processes a business puts in place to create a workflow of all paperwork, files, records, and information.

It generally includes considerations for every aspect of a document's life cycle, from creation to eventual destruction.

There are dozens of ways to go about finding a way to optimize your office for effective document management but to make sure that you have your bases covered, there's several factors that you need to consider:

- The size of your office
- The laws and regulations that your company has to follow
- The type of system you want to implement
- How sophisticated you want the system to be

Here are eight steps that should be the mainstays of a solid document management program:

Step 1: Conduct a Complete Inventory of All Documents

By doing a complete inventory of all the records you want to manage, you can implement the right processes and the proper staff to maintain and improve your program over time.

Step 2: Determine who is going to manage the process

Define what steps of the process need to be managed, and who is going to manage each step of the process to ensure your process is sustainable.

Step 3: Develop a Retention and Destruction Schedule

Create a program that allows you to review, identify, and monitor the various retention times for all the documents received or created in the course of regular business activities. A retention and destruction schedule helps maintain and contain guidelines for how long certain documents should be kept and, how they should be destroyed.

This helps eliminate the risk of older documents causing legal problems, and will save you money by reducing storage costs by shredding documents that are past their useful life.

Step 4: Determine the best way to store and manage your records

Most companies use several different systems to store and manage their records depending on the type of business that they're in and the workflow of their office. A bad investment in the wrong system can lead to bad records management– and more headaches for your business.

Some companies prefer an electronic document management system and a cloud storage service, eliminating the need to store paper files. All their documents are scanned and indexed, making them easier to manage and find.

Other companies prefer to utilize a hard-copy storage system through a records management company and secure off-site records storage to manage their files. That way, they have access to their documents any time they need them, and still maintain hard-copy records for legal or regulatory purposes.

Step 5: Create and document proper procedures

Create systematic procedures to ensure your program can be followed and documented easily. Think of this like an instruction manual- the more detail the better!

Step 6: Create a disaster recovery plan

Accidents happen- create a disaster recovery plan to help eliminate issues in case of a natural disaster, fire, flood, or worse. Have a solid backup system in place as well.

Step 7: Training and Implementation

Training and implementation are the most important aspects of implementing a document management plan. Having well-defined processes and procedures in place will come in handy in case of turnover or retirement.

Step 8: Maintaining and auditing the program

Once the system is implemented and you've completed all your training, it's important to document any issues or inefficiencies that occur. Updating processes and auditing procedures will ensure that you correct any bottlenecks as quickly as possible.

Utilizing these steps to set up your program will put you on the right path to developing a document management plan that is flexible, manageable, and tremendously valuable to your company.

Once you have a document management system in place, the next step in the process is to identify and develop a document retention and destruction plan.

A document retention program provides for the systematic review, retention and destruction of documents received or created in the course of business.

It identifies documents and business records that need to be maintained and contain guidelines for how long certain documents should be kept and how they should be destroyed.

Why You Should Implement a Document Retention Program

A document retention program is important- it can protect you in litigation and help ensure compliance with federal and state laws and regulations.
Evidence of a clear and consistently enforced document retention program, enacted for valid purposes, will go a long way to convince the court that the destruction of a document or business records was reasonable.

Tossing the wrong paper or deleting an important e-mail can also have bad consequences. Not having a document can mean the difference between winning and losing in a lawsuit.

There are four principles to balance when creating a records retention program:

1. Is there a legal requirement for keeping the document, including federal, state, and local laws?
2. After the document is past its useful life, is there any purpose could it serve? Could it be used to support or oppose a position in an investigation or litigation?
3. What is the consequence of not being able to locate the document?
4. Can the item be *reliably* reproduced elsewhere if needed? Is the information available from the public library, an online source, a database, or company central files?

Once you have developed your program, you need to consider how and where you want to store all the files you mange.

All documents should be stored in a secure location that is climate controlled and includes a fire suppression system. This is why companies outsource their storage needs to a secure document storage company. They can provide the secure storage and record backup services and even help you index your files for easy retrieval.

Now that you have a document management and retention program in place, you need to consider the best ways to prevent corporate espionage and identity theft. It all starts by tightening down your security protocols and it all ends with proper document disposal.

Shore Up Your On-site Security

When you have thousands of records, files and documents in one place, implementing security measures can be a nightmare.

The first thing we recommend is to take each file type and category and classify them based on the type of risk that your company can be exposed to if that information was exposed.

By assigning different levels of security based on how critical the information is, you will be able to quickly figure out how to classify each record to determine if it needs to be stored on site, archived off-site, or securely destroyed.

Once you've determined what record goes where, you can move on to the different steps you can take to secure the records you choose to store onsite.

There are several different risks to consider:

Operational risk: If these records are compromised, will your company be unable to meet operational goals and objectives?

Financial risk: Does the loss or theft of these records affect the ability to protect and document financial decisions or expenditures?

Reputational or image risk: If these records were released to the public, would it cause the company to lose their status as a reliable, effective, and accountable company?

Physical or security risk: Do these records contain sensitive information that, if in the wrong hands, could cause loss or damage to employees, the company, any physical building or office?

Once you have classified all your documents, you need to take steps to ensure that anything that might be a risk if it's compromised is secured. There are several ways your company can do to minimize the chance of a hard copy data breach- here are some items that you need to consider:

- **Lock Everything Down**

  If you need to ensure that some documents remain secure, you should lock the drawers, the cabinet, and the room. Not only are they a deterrent for an employee with prying eyes, they can also stop someone from actually breaking into the cabinet to take or copy files.

- **Install Fire and Security Alarms**

Fire alarms and security alarms are vital to ensure that you can minimize the risk of a fire consuming all your documents, and reduce the chance of someone infiltrating your documents room to obtain company secrets.

- **Limit Access to Your Critical Documents**

How many employees have access to all of your company documents? Limiting who can access, re-file, and copy company documents helps eliminate human error, which could include accidentally losing documents, taking documents offsite, having extra copies of critical files around the office, or even corporate espionage.

All your documents are handled and disposed of properly by employees that have the clearance level to read the contents of every file they handle. The smaller that number is the better.

- **Label All Documents, Files and Cabinets Appropriately**

Misfiled or misplaced documents cost your company money. Whether you have to search for it or reproduce it, you have to factor in the cost of the time it takes to find or reproduce that file, along with the additional chance that the information may be compromised. Make sure that all your documents, folders, drawers, and file cabinets are labeled clearly and properly.

- **Conduct Regular Audits**

Once you have a documents management system in place, you need to make sure that the system is maintained. Schedule regular audits of your critical documents will help you maintain version control and reduce the chance of a data breach since you have a better chance of catching when something valuable is missing.

- **Destroy Your Documents Securely- and Document When You Do**

Once you have determined how you're going to manage your documents, you need to make sure to adhere to your document retention plan, and take the time to destroy your documents properly and securely as they pass their required retention time.

Destroying (and properly documenting) all your documents help to reduce legal liability, reduce the amount of documents you store onsite, and protect your critical documents from getting into the wrong hands.

Shred Your Documents Securely and Regularly

Document shredding is a critical piece of any document management plan. It's critical to make sure documents that have personal, financial, or sensitive business information are retained as long as they need to be.

Once a company is no longer required to hold on to them, documents should be securely shredded to limit liability and free up storage space.

One of the biggest questions to consider is what documents should be destroyed- and who makes that decision. Implementing a shredding policy where certain documents are destroyed can be effective.

Secure bins are placed in common areas and employees are allowed to determine what documents need to be shredded, and which documents can just be recycled. It gives a sense of security and ensures that most of the documents that should be destroyed are disposed of properly.

There are several different methods that you can consider to protect your company from a low-tech hack, where hardcopy documents are compromised by not being shredded properly, left out in the open or duplicated without keeping track, or just simply thrown away or misplaced.

Mobile Shredding is one of the best methods to ensure your documents are shredded properly. It's almost exactly what it sounds like.

First, you contact a shredding company, and they provide secure, locked bins where you can place documents that you need to shred until they're full, or until you reach your agreed-upon shredding pick-up date.

When you're ready to have your documents shredded, a shredding company will schedule a time for a mobile shredding truck to come out to your office to shred the documents right at your location while you watch.

Mobile shredding gives you more flexibility and eliminates the need to transport heavy boxes to a drop off location. It also can provide a consistent and reliable shredding schedule for a business.

Check out some of the advantages of mobile shredding- maybe it'll help you determine the best solution for your project.

- **You can watch them shred your documents**

  If you have sensitive documents, mobile shredding could be the answer for your shredding project. All your documents are picked up in secure, locked containers and shredded right there while you watch. There is no physical contact between the shredding contractor and your documents at any time.

- **You can easily schedule regular shredding jobs**

  One-time purges have their advantages, but to prevent legal liability and data breaches, you should really have a shredding management plan in place to ensure that you're protected. A mobile shredding service can schedule ongoing pickups to prevent the buildup of unsecured information and eliminate the chance of a low-tech hack.

- **You have negotiable instruments**

  If you have any documents or items that can be exchanged for cash, you need to make sure that they are destroyed. This could include coupons, unused checks, certificates, and more. Mobile shredding ensures that these items don't fall into the wrong hands.

- **You don't have to leave!**

  The biggest advantage of mobile shredding is that you don't have to take time out of your day to have your documents shredded. Most mobile shredding services will pick up and shred all your documents for you.

  All you have to do is call, and schedule a time to have them take care of it. Not only is it secure, it eliminates hassle and takes multiple steps out of shredding your documents.

  If you have a large amount of documents, or are looking for an option that is slightly cheaper, offsite document shredding might be the answer.

Offsite Document Shredding is when a professional shredding company picks up your documents in locked bins and transports them to be shredded in a secure facility.

This service allows you to have your documents picked up and transported to a secure facility, minimizing the risk of a data breach or security issue and the chance of a corporate spy or internal employee theft that can compromise your business.

The actual benefits of offsite shredding mirror mobile shredding, but eliminate the cost of having an actual shredding truck come out to your location. This service is geared toward companies with a large amount of documents to shred.

Offsite shredding can save you anywhere from $1 to $2 per box by using an offsite shredding company (but those prices vary depending on location and provider). You also benefit from the co-mingling of shredded documents.

By including your shredded documents with dozens or hundreds of other companies, it makes it virtually impossible to separate and re-assemble shredded documents before they are pulped, recycled, and made into new paper.

Either of these shredding options gives you a secure, reliable way to dispose of your documents and minimizes the chance that your company will be a victim of corporate espionage, identity theft, or fraud. Document shredding companies take significant steps to ensure that your information is protected.

Another extremely effective option to ensure sensitive documents are destroyed securely and properly is to implement a Shred-All Policy.

What is a Shred-All Policy?

It's as simple as it sounds- once a document is no longer useful or necessary, it's shredded. That way, there's no question about what type of document needs to be retained.

It leaves little room for a data breach, and provides a simple solution to what can become a complex problem by eliminating a decision-making process on what to shred and what not to shred.

If given the choice, it's always wise to error on the side of caution, which is why a Shred-All policy makes sense. There are several reasons to implement this policy in your company.

A Shred-All Policy takes these types of mistakes out of the equation by removing the requirement to make those decisions so that no one in your company makes a mistake that costs you hundreds of thousands of dollars.

Here are some other advantages to implementing a shred-all policy in your company.

- **Less Risk of Security Breaches**

  Every company should do everything they can to eliminate data breaches. It could cost your company hundreds, even thousands of dollars. 40% of data breaches related to paper documents are due to an employee making a mistake. Eliminating the chance of error makes a whole lot of sense.

- **Compliance**

  Identity theft and corporate espionage is a growing problem for businesses. Accidentally exposing your customers or employees personal information comes with grave consequences. If you're a small business owner, there's a chance that you could lose your business with just one breach. Besides the business risks, there are also specific laws and regulations to protect consumers and ensure that personal information is protected.

  This will help your company comply with all the complex laws and regulations of your industry- since all documents are destroyed after their appropriate retention times, you eliminate the need to update these policies as current laws change or new laws are added.

- **Training**

  Educating your employees to make a decision on which document(s) need to be shredded takes time and money. Every time the policy changes, a training session needs to be in place to make sure that you don't have a security breach.

  You also have to consider the time and effort it takes for managers to ensure the policy is being enforced. Wouldn't you rather have them working on growing your business and improving your employee's performance?

  That's the beauty of a Shred-All Policy.

  - **It's easy to teach.** Once you're done with it- shred it.
  - **It's easy to enforce.** Shred your documents. Don't keep them.
  - **It's low maintenance.** Eliminate costly training sessions and free up your manager's time

  The most important thing is to make sure your policy is enforceable. By having an employee sign a document stating they understand the policy, you have a way to hold them accountable if they don't adhere to it.

If you have a lot of documents that need to be retained, or aren't sure which shredding service to choose, you should consider offsite document storage- it will free up office space, maximize your document management plan, and secure documents without making them difficult to access.

Utilize Offsite Document Storage Management

Document shredding and internal security shouldn't be the only considerations for your company.

You need to have a way to store documents that need to be retained for a certain period of time, and another option to ensure that company secrets and information isn't compromised.

That's where offsite document storage can help you- by utilizing an offsite document management company, you increase the accessibility of active documents in your office, and ensure that archived and critical documents are protected from theft, natural disasters, and corporate espionage.

Document storage is a great alternative to a shred-all policy- it gives you a way to hold onto all documents you need to while freeing up office space and giving you access to archived documents quickly and easily.

There are tremendous benefits to utilizing offsite document storage:

- **Offsite Document Storage Saves Space**

  Besides having to sort through paperwork manually, on-site record storage takes up valuable office space. To free up office space and make it easier to find documents, you can hire a company to scan your documents into an electronic system, or use an offsite storage facility where it may be cheaper to keep business records.

- **Increase Security by Storing Documents Offsite**

  A business keeps proprietary and confidential information. Onsite storage can create security problems and give access to these records to employees or people who should not have access.

  By moving records to an electronic document management system or offsite records storage, the only people who can gain access to these documents are those previously authorized to do so.

- **Document Retrieval is Easy With Time-Saving Search Features**

  Before sending your records to an offsite storage facility, they are cataloged, categorized, and imprinted with a bar code that identifies file contents. This information is added to a storage company's database, which makes it easy to search for needed records.

  Instead of having to search through countless file boxes to find archived or important documents, simple computer search features allow quick and easy access to documents.

- **Protect Against Natural Disasters**

  One of the most important features of using an offsite storage facility or electronic document management company is the protection offered to businesses' most important documents.

  If catastrophe strikes in the form of earthquakes, weather problems, floods or other unforeseen disasters, your company's important documents are safe and secure.

CONCLUSION

Protecting your company from external threats is a top priority. With billions to trillions of dollars lost every year due to fraud, identity theft, and corporate espionage, the only way to ensure your company is safeguarded is to take the proper precautions and implement security measures and procedures for every step a document takes throughout the company.

1) **Start with a solid document management plan**- detail what types of files you have, where each file goes in the company, and how secure each file needs to be.

2) **Create a workflow for long-term document retention** (either internally or with an offsite document management company), and make sure you track when a document is past its useful life and needs to be destroyed.

3) **Lock down your internal documents**- this creates bottlenecks for corporate spies and identity thieves to get to your information, and make sure you have security measures in place to prevent low-tech hacks.

4) **Have a plan for disposing of your documents**- implement a shred-all policy, or hire a shredding company to come to your site and pick up all documents that you want shredded.

The more you plan, audit, adjust, and improve your systems, the more you reduce your chances of being negatively affected by a data breach, corporate theft, or the victim of fraudulent activity on behalf of your company.

There's nothing worse than bad publicity from a data breach that affected thousands of customers and exposed them to identity theft or a fraudulent mail piece that tarnishes your brand.

ADDITIONAL RESOURCES

Identity Theft: Surviving the Crime of the Century

Run of the mill identity thieves are still low-tech- dumpster-divers looking for blank checks, credit card receipts and bank statements, which can be easily negotiated on the streets for drugs or chump change. But today, most identity thieves have gone high-tech.

Six Simple Steps to Protect Your Employees Identities

Here are 6 simple steps that every company should take to help keep their employees information safe from identity theft.

Shredding Helps Prevent Corporate Espionage

Even though the days of dumpster diving for information are winding down, corporate espionage is still a major factor in business today. There's several ways a corporate spy can infiltrate your company- take the proper steps to avoid this from happening.

10 Things Corporate Spies Don't Want Shredding Contractors to Know

There are two types of corporate spies: your competitors that spy on you, and "unfriendlies" that spy on your clients. As a business owner, you must guard against both types from violating your security protocol. Here are 10 things they don't want you to know.

Prevent Fraud with Proper Document Management

Fraud is a huge problem for individuals and companies- there are information thieves that send out mail, email, and even online advertisements that try to take advantage of trusting customers and employees. Here are some of the things we recommend to ensure you have all your bases covered to prevent fraud on behalf of or inside your company.

Sources:

Personally Identifiable Information
https://www.fbi.gov/scams-safety/fraud
https://en.wikipedia.org/wiki/Industrial_espionage
http://www.inc.com/will-yakowicz/stolen-trade-secrets-cost-us-480-billion-a-year.html
http://www.creditsesame.com/blog/staggering-costs-of-identity-theft/
http://www.pymnts.com/news/2015/2014-fraud-spike-cost-u-s-retailers-32-billion/
UN's definition of the various levels of risk

FOR MORE INFORMATION

For more information, please contact info@shrednations.com