

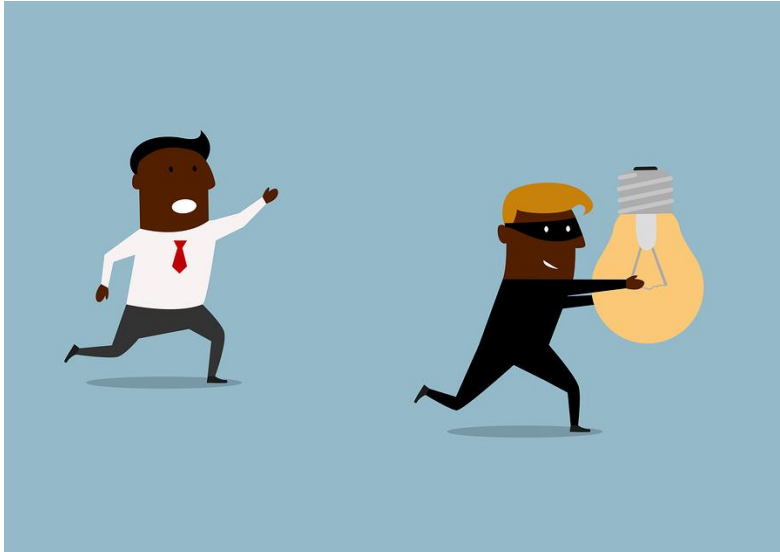
The Benefits and Cost of Utilizing Offsite Data Storage

Record Nations | @RecordNations

Table of Contents

Introduction	3
Data Breaches in the News	4
Data Vulnerabilities—and How to Protect Your Business	5
Defending with Offsite Data Storage	8
Pros and Cons of Hard-Copy Storage	8
Pros and Cons of Digital Data	11
Conclusion	13
Additional Resources	14

Introduction



Over the course of 2014 and 2015 alone, data breaches in industries from restaurants to the healthcare system were shaken to their roots by the heavy blow of hackers and identity thieves accessing, manipulating, and distributing both businesses and customers' most private of information.

Though hackers slipped past different company securities in a variety of ways, the same fact

still remains—protecting from data breaches is a continually growing concern for business owners and consumers alike.

Besides just payments and card numbers, critical personal information of consumers has also been made vulnerable, driving both investors and customers alike away from companies with seemingly unstable data storage and into the arms of their waiting competition.

While some have floundered in the ensuing chaos, other business owners have faced the new challenge of protecting their data and preventing data breaches in new ways using both hard-copy and digital strategies for storing their information securely. Although each comes with its own advantages and downsides, the benefits of company data security generally far overshadow.

Not only will this article help to identify the most common data vulnerabilities in businesses today, it will also advise and assist you with strategies to help bolster your own business data management and storage while preventing a data breach as well.

After developing strategies and practices for preventing a data breach of your own business, Record Nations can assist you in finding local providers offering record storage and management services in either digital or hard-copy formats to best suit your company needs.

Data Breaches in the News

Although no one likes to imagine the worst, in early January of 2014, what seemed a bad dream became a reality for apparel designer Neiman Marcus. Headlines broke on the story of a major credit and debit card breach of the company, where over a span of three to four months a malicious software program had been installed in company card readers to collect payment data from shoppers. Eventually affecting as many as 350,000 cardholders, even a large company like Neiman Marcus took a hit of \$134 million in profit losses during 2014 due to the size and scale of the data breach.



Upping the stakes significantly, in early 2015 health insurance company BlueCross BlueShield reported the discovery of a data breach that went on to affect as many as 11.2 million subscribers and business associates of the company. Despite warnings to the insurer of its IT systems and department being less than secure in the event of a possible threat, unfortunately the personal information and data of customers—including Social Security numbers, addresses, and bank accounts—were made vulnerable and available to hackers.

While the impact of these serious blows to a business may seem short-term, lasting largely until the breach in data security is patched, even the most massive and well-known companies and organizations potentially face a long-term fall in reputation and credibility that may never be fully recovered. In a world where more and more information is stored, and especially digitally, ensuring that your company data is secure is all the more critical to preventing the loss of both company credibility and customers. As a result, it's imperative that as a business owner you are aware of the most common data vulnerabilities among modern businesses today.

Common Data Vulnerabilities for the Modern Business



No matter your company's size, there are countless risks and vulnerabilities to a data breach that can be hard for a business owner to completely account for. If you have employees you allow to work from home on digital documents, work laptops and USB sticks can be easily misplaced or stolen, quickly jeopardizing critical company data.

Similarly, maintaining hard-copy data storage can also lead to increased chances of a data breach. Small businesses that have little enough paperwork that they don't use digital storage as a primary method of data storage are then faced with the problematic question of how to manage their information.

So, when it comes to preparing and protecting your company in the event of a data breach, many business owners may wonder where to begin. To answer this and better familiarize you with some of the most frequent causes for major business data breaches, the following are a few of some of the most common causes for breaches in many company security systems today:

Inside Job

While most consider attackers to be an external threat, business owners may be surprised to discover that one of the most common causes of company data breaches is actually when a rogue employee causes internal damage. With already working knowledge of the company data and network systems, there is potential for quite a bit of damage done before proper action or authorities can be notified in time to stop it.

Employees Not Knowing Better

While a malicious insider attack from an employee in your company may at first seem like the worst-case scenario as far as employees go, an employee who accidentally leaves an unlocked work briefcase or laptop on the bus seat can be just as likely to cause a catastrophic data breach. Without employees having proper and up-to-date document and data security training, there are potential liabilities behind each desk in the office.

Third-Party Services

When businesses enlist the assistance of third-party providers for transactional services, like credit card readers, some service providers may not meet the same security standards that your own company sets for itself, effectively lowering both your guard and theirs to the threat of a data breach. Even if their credentials are stolen at another company the provider serves, poor security practices on their part can still expose your own company to a potential threat.

To help prevent the possibility of your precious business information falling into the wrong hands or being improperly destroyed in the event of a data breach, many business data and record management experts highly recommend the services of a third-party offsite data storage and protection company. Specializing in the security of either your hard-copy or digital company records and information, these businesses can both help to save your company long-term money and potential headaches by covering any and all gaps in your data security.

Besides offsite record storage providers, data security experts also suggest that business owners themselves be brushed up and stay up-to-date on current security practices to be able to maximize your company protection.

Protecting Your Business from a Breach

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 from data breaches in use today. Safeguarding both company and customer data is both a critical and constantly evolving practice. Although it may seem to be a daunting task to try to identify and close any possible gaps in your data defenses, following this short list of tips and strategies alone can give your business a major boost in the right direction:



Look Outside the IT Box

To ensure that your business is secure from top to bottom, data and other information security must extend beyond just the IT department. For instance, it is important to consider data storage practices regardless of whether the company tends to favor either digital or hard-copy information management services offsite.

Minimize Opportunities for a Breach

From the top to bottom of your organization, keeping straightforward catchall rules for how your business decides to keep and manage information can also 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 potentially lose as well, effectively shrinking any sort of target a data thief may have aimed at your company information.

Generally speaking, it can be broken down to simply reducing the amount of information you store and the places you store it. Only give sensitive data access to trusted employees, and be sure to keep records of which employees and data security companies are given any access to information.

Be Prepared for the Worst

Owners and managers specifically use this policy standardization not only to make data management easier and more organized, but also so that both new and existing employees are taught to consistently uphold the same data-protection policies company-wide. In the event of a data breach, be sure that your company has an [data breach recovery plan](#), and that your employees are well-informed of what to do in case of emergency.

Seek the Assistance of Data Security Experts

An evaluation performed by an objective, neutral party leads to a clear and credible picture of what's at stake, without pressuring staff who might otherwise worry that their budgets or careers are in jeopardy if a flaw is revealed.

Furthermore, research shows that organizations with a strong security posture or a formal incident response plan in place prior to the incident can reduce the average cost of a data breach by as much as \$21 and \$17 per record, respectively.

Every business has records to store and manage to some extent, and no matter the size of the company, data storage services are a critical investment for keeping your business secure.

Defending with Offsite Data Storage



From massive corporate superstructures to small office spaces, enlisting the services of a third-party company that specializes in nothing but the protection of business data can vastly minimize the potential for a catastrophic data breach shaking your business to its roots.

Considering that by doing so it relieves both the pressure of securing data or worse yet, losing your valuable company information due to an information breach, record storage in either offsite hard-copy or digital formats has become an incredibly common business practice today.

Advantages to Hard-Copy Offsite Storage

Although digital data storage technology has begun to expand in its widespread use across all industries for sake of its convenience and ease of accessibility from numerous locations, this can also be its Achilles when it comes to the possibility of a data breach if a hacker were inclined to copy all files within reach.

While old-fashioned, this is where hard-copy data can come in handy, providing some unique advantages over new digital data storage technologies, including:

Still Find Your Files Fast

Much like your local library, even though many of the documents and data you may be storing at an offsite location are still in their physical hard-copy form, modern technology and barcode management systems allow for individually labeled files to be quickly and easily found at your convenience.

Since your hard-copy data is not just stored at an offsite location but also organized and managed for you as well, this can give you some helpful insight into the state of particularly critical business documents. Every time either you or a client potentially needs one of your files in storage, you can safely rely on the third-party service to dispose of old and unnecessary documents and be able to provide you with up-to-date versions of your documents

A Cleaner, Organized Office Space

Trying to manage company data in-house even in digital formats can become somewhat messy when there is a large amount of information or many

individuals involved with its storage and management. Hard-copy storage can become even more complex when the actual floor space needed for a file cabinet must be also factored into the equation. Considering the average 15–20 square feet needed for just one set of cabinets, an already small workspace will benefit tremendously from the extra room.

Doesn't Make for a Sneaky Data Breach Getaway

By maintaining a set of secure hard-copy files and an emergency plan in case of a breach, business owners can at least potentially have less to lose in a situation. Even if security is compromised, hard-copy records and data cannot be quickly and easily reproduced by hackers, giving time for a proper response to minimize possible losses or damages sustained.

Hard-Copy Offsite Storage Downsides

In a world where digital technologies are slowly but surely coming to replace the written word, many may soon wonder about the future fate of hard-copy document storage on a company-wide basis. While there certainly are some upsides to offsite hard-copy data management, there are also some drawbacks:

Falling Behind Future Digital Formats

Early-on, converting hard-copy files and data to digital formats could become tedious, as new technologies with more efficient storage were constantly emerging. Today however, digital file formats are widespread and for the most part far simpler to update, as digital information security constantly evolves as well. Consequently, now making the move of all your hard-copy data to an offsite location for constant protection is a much less attractive option, as it leaves little room for an easy change of plans later on.

Ease of Access (Or Lack Thereof)

While an offsite storage site for hard-copy data and files for company can be an excellent way to free up room and reduce clutter in your daily workspace, this advantage may actually have a limit depending on how frequently an individual piece of data may need to be referenced or used by your business. Even though the file is effectively protected from



theft or destruction, access to a special offsite file could end up being a detriment

to the efficiency of a workplace when the time simply to retrieve the data is factored in.

Fire Hazard

Although odds tend to be slim, a chief safety concern among offsite storage locations for hard-copy documents revolves around the threat of fire. With this in mind, many go to extreme lengths to assure customers of fire-suppression systems installed, however business owners should still keep this possible danger in mind since offsite storage locations charge for storage based on space. Generally, only a single hard-copy version of sensitive company data or information is stored at these locations, meaning that in the event of an unforeseen incident at the actual offsite storage location, your data could be effectively destroyed. For extremely important documents your business cannot afford to lose, consider keeping another backup copy in a secure place in the office, just in case.

As you can see, there certainly are some perks to opting for hard-copy offsite data storage for your company, especially when it comes to highly sensitive information that if digitally compromised, could be quickly copied and distributed in digital file format among the wrong people.

Alternative to hard-copy documents and what has traditionally been the method of record keeping for most of the 20th century, electronic data storage now offers advantageous opportunities for managing your company records and documents—but with an additional bit of responsibility for safekeeping.

Advantages of Digital Document Storage



More and more frequently, businesses across varying industries are beginning to adopt [electronic document management systems \(EDMS\)](#), in favor of classic hard-copy documents filling up box after box with files. Even when these boxes of said files are transported to an offsite location for storage, they can be hard to access remotely, making the convenience of digital data even more attractive.

If in an ideal world, you'll be able to store your business documents and files in a secure location while still having the freedom to access your data at will, then digital data storage may be the direction to take your business in. The following are a few of the top benefits that come along with embracing technology and digital record storage:

Bonus Storage Space

Hard-copy paper documents take up space, no matter where you eventually decide to store them, and even if you decide to opt for offsite hard-copy data storage to free up space in your own work area, offsite storage locations charge their customers based on the space they use. On the other hand, however, business owners are also offered the alternative option of pursuing digital data storage, where with the help of only a scanner and thumb drive, banker's boxes full of files will seemingly begin to disappear.

Access Your Files on the Move

Although an offsite hard-copy storage facility may be able to use a barcode system for cataloguing the documents you store, this still pales in comparison to the accessibility of digital storage. Not only can digital documents be quickly and easily sorted, organized, and location via keyword searching, accessible digital document management methods like cloud storage also allow for a company's files to be available on-demand, making it easy to both reference and store information as necessary.

Downsides to Digital Document Storage

Despite the many perks revolving around the ease of access to digital data storage, this accessibility can be both a curse as well as a blessing depending on the type of business

you're running and documents you're storing. Here are a few of the chief-most considerations to keep in mind:

Keeping Confidentiality King

When it comes to legal or financial documents that include official and notarized signatures, there is slightly more risk involved in storing these in a digital format. As mentioned before, digital documents can be quickly and easily reproduced, and unless a file containing sensitive information is protected with a password or other [data encryption techniques](#), probabilities of this falling into the wrong hands are much higher.



Who Else Can Access Your Files Remotely?

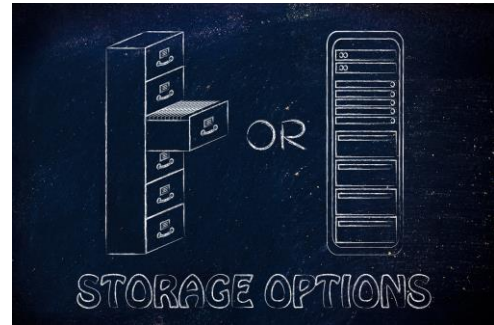
Although digital data storage opens plenty of opportunities for a critical piece of information to be quickly located and collected by the business owner or other company employees, digital document storage also allows for a fairly wide audience who can access the file—including potentially those trying to manipulate the file.

Conclusion

Depending on the business and its overall size, business owners are faced with several options for how to manage and store company data and documents without wasting any of their own precious space in-office.

Although there generally are numerous factors to consider, at the end of the day the essential point that must be kept in mind by business owners is what your specific business needs for data storage are. Some of the most common questions to answer:

- How big is your company, and/or how many of your employees will need regular access to company data and other files besides just you?
- What would be the worst case scenario *if* your company files were to be compromised?
- Do you want employees to have limited access to data, or will you plan on additionally educating employees on the dangers of company data breaches?



There are pros and cons to both digital and hard-copy data storage methods, but at the end of the day, a final decision must come down to your own unique business circumstances. For small companies with records that simply must be retained, a hard-copy storage system may be all that is necessary, but the larger the company and the more information needing to be stored and referenced regularly, the more attractive digital data storage becomes.

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

To learn more or for further assistance deciding for your company, feel free to contact us—Record Nations can help to set up business owners with reliable [document storage and management services](#) in your area. **Fill out the form to the right, or give us a call at (866) 385-3706 today!**

Additional Resources

[Record Storage and Retention Laws](#)

Privacy concerns and new document retention laws have made record storage management a top priority for companies nationwide, and at Record Nations we do our best to keep you up to date on any changes to laws that might affect your document storage. Learn about all the laws related to record storage and medical Storage, including HIPAA, FACTA, GLBA, and more!

[Pricing Out a Scanning Project for Your Business](#)

Document scanning is changing the way companies manage and utilize their files. If you are the owner of a primarily paper-based business that's hoping to make the digital conversion to document scanning, check out Record Nations' guide to pricing out a scanning project.

[Cloud Backup, Storage, and Electronic Document Management Systems \(EDMS\)](#)

Storing and/or backing up your files and critical data offsite from your corporate office is one of the best ways to prevent data loss and eliminate the clutter of paper documents. Learn more about the different digital data storage options available for your business!