PLANNING FOR BUSINESS IDENTITY THEFT & DATA BREACHES

THE GUIDE TO PREVENTION

SEPT 2016

Record Nations®

777 S WADSWORTH BLVD 3-250
LAKEWOOD, CO 80226

RECORDNATIONS.COM

BUSINESS IDENTITY THEFT AND DATA BREACHES – WHAT'S THE DIFFERENCE?

BY RYAN MCHUGH

In the modern business landscape, external threats are everywhere—ranging from hackers and data breaches resulting in valuable customer information being lost, to identity thieves taking advantage of a company identity to reap rewards at others' expense.

With potential destruction that can range from costly fines to years of restoring the company's credit or even public image, no reasonable business today should go without taking the proper steps to protect themselves and prevent the possibility of such an attack occurring.

So now you must ask yourself—what steps has your company taken to securely store information and protect itself from electronic threats? Here, you can find all the information and details you need to be sure your company has all of its security bases covered.

While in the past the phrase "data breach" may have seemed foreign to the average person, today the term frequently crops up in headline news stories as incident after frightening incident of companies losing customers' credit card numbers occurs by the thousands.

Launched into the public eye by extensive data breaches sweeping across massive companies like Target, Home Depot, and Anthem, the public is more than aware of these attacks that threaten both the companies they shop at and the personal information they provide there.

However, there are also other threats that should be on a company's radar—types of attacks such as business identity theft which often receive far less attention than high-profile data breaches, but are nevertheless just as important to prepare for.

Today, individuals are no longer the lone targets of identity thieves. Instead, companies must also be on the watch, as criminals will now steal and use the identity of a business to establish lines of credit which extend farther than the average individual—leaving the damage to a business's own credit history all the more severe.

Regardless of the method of attack, the potential consequences and long-term impact of both business identity theft as well as data breaches can be severe.

Throughout this white paper, we provide not only an in-depth guide to data breach and identity theft prevention strategies to help companies securely manage their sensitive information, but also include several key points to include in all your data breach and identity theft recovery plans.

TAKING THE FIRST STEPS: CREATE A DOCUMENT MANAGEMENT PLAN

Considering the fact that in today's world of easily-accessible information a single document sent to the wrong inbox or discarded in the wrong bin could lead to a company's identity being stolen or their entire systems being breached, the need for establishing sound document management plans is essential.

With a document management plan, businesses create a comprehensive policy for managing and storing their information, detailing the recordkeeping process as well as the lifespan of documents from the moment of their creation to the second they are securely destroyed.

Besides merely the importance of organization—especially for larger companies—well thought-out document management plans are an ideal way for a business to always keep its finger on the pulse of its securities.

A large percentage of breaches and stolen information incidents are caused by simple mistakes and human error, but when a document management plan keeps a constant eye on the status of all documents—these errors can be caught before they lead to disasters like corporate identity theft and data breaches.

Common components of document management plans typically include:

1. **Conduct a complete inventory of all currently-existing records**
2. **Designate a single employee or manager with responsibility for the record management process**
3. **Develop a record retention and destruction schedule—typically with varying retention guidelines by state**
4. **Evaluate and determine the best method(s) for storing and managing records**
5. **Create, document, and establish proper company procedures for record storage and disposal**
6. **Implement your policy, train employees, and ensure constant communication throughout the company on any procedural changes**
7. **Create a backup disaster recovery plan in the event of a breach or other emergency to immediately minimize damage**
8. **Maintain, audit, and optimize prevention and recovery plans to maximize efficiency and effectiveness**

With the necessary recipe for creating a secure and thorough document management plan in mind, many companies may quickly reach steps 4–5, but then stop to wonder—what are the actual options for storing and managing company records?

To help answer this common question, here we provide the top strategies other businesses currently employ for record storage in order to give companies the big-picture perspective they need when making major business decisions:

SCANNING RECORDS

Given the fact that so many business identity theft and data breach incidents stem from cases of records being misplaced or improperly destroyed, many companies have turned to embracing the power of technology and managing their documents digitally.

Scanning and storing documents using electronic document management systems or other digital options allows businesses to greatly simplify the process of tracking and managing a live index of their records, in turn reducing the likelihood of the wrong document slipping through the cracks in company defenses.

Any document scanning conversion process for a business is a simple one. Once the document is run through a scanner and converted to a digital image, it's indexed and organized to make it easier to find.

Afterwards, the files can still be made editable using what's called Optical Character Recognition software (OCR)—meaning no compromise must be made to scan and convert a company's records to convenient and space-efficient digital documents.

With the ability to search for specific documents and keep an entire file cabinet's worth of records on a single hard drive, the choice to upgrade to electronic options can often be boiled down to as simple a business decision as investing in a car or instead sticking with the traditional horse and buggy to get around.

CLOUD STORAGE SERVICES

Compared to alternative document management systems, cloud storage services are often an ideal option for smaller companies opting for digital record storage strategies.

Cloud storage systems are generally hosted in an offsite data center operated by the storage provider. By storing records on a cloud-hosted system, a company can access documents from anywhere and at anytime using an internet-connected computer, tablet, or mobile device.

Storage providers typically back up all company data regularly, so remote access to up-to-date information is always available. To ensure all information sent over the cloud storage server is secure at all times, many providers also include services such as SSL data encryption for all information as part of their fees.

Since cloud storage is a leased software with ongoing payment plans, one of the greatest appeals of the service to small business is its affordability when company finances cannot otherwise support the IT staff and resources necessary for a custom system.

Providing all the needed infrastructure to securely store digital records and lower the odds that a misplaced company document will lead to the next identity theft or data breach story on the nightly news, cloud storage services offer a cost-efficient and convenient option for small business record storage.

ELECTRONIC DOCUMENT MANAGEMENT SYSTEMS (DMS)

The alternative to cloud storage options, companies also have the option of using electronic document management systems (DMS) for record storage.

While cloud storage is handled offsite by a provider, the difference for a DMS is it requires an in-house IT team to manage the system, as a DMS usually must be custom-built to meet the needs of an individual company.

Since the system does not require a constant internet connection, one of the greatest advantages to a DMS is often its speed—especially when it comes to large companies.

Having a custom-built framework for the system also allows room for extensive customizations including not just space for security add-ons such as firewalls and data encryption, but also features designed to maximize the accessibility and efficiency of the system.

OFFSITE RECORD STORAGE

For businesses needing to retain certain hard-copy documents they don’t use or need frequently but must retain for legal or other security reasons, there is still a crucial need for secure and space-efficient storage options.

This can often lead to problems for businesses, as managing these records in-house means that valuable office space must be used for file cabinets. Furthermore, productive employee time must be spent maintaining documents, and there is still the chance that the records could be misplaced, stolen, or destroyed in the event of a fire.

With offsite record storage services, however, these concerns and inefficient expenses are all eliminated in one fell swoop.

Besides providing access to company documents at any time to ensure businesses aren’t sacrificing accessibility for security—including emergency retrieval services for unexpected situations—offsite record storage offers all the same advantages of storing documents in-house, but with a few extra benefits of its own.

ID THEFT AND DATA BREACH RECOVERY TIPS

Although a company should take all preventative measures available to protect themselves from the possibility of a data breach or business identity theft occurring, no realistic company should hope for the best case scenario without first planning for the worst.

As the rates and overall damages of these incidents have continued to trend upward with recent years, many companies as a result are strongly encouraged to look ahead and create a data breach recovery plan to outline how the company would respond if disaster *were* to occur.

A business bungling their response to an attack resulting in the loss of customer information can inflict crippling damages to a company, which range from simply the resources needed to remove or restore compromised records, to the poisonous public image they will present in not being able to protect their sensitive information.

The following is a breakdown of how to properly handle an attack and the necessary components of every data breach recovery plan:

ELIMINATE ALL THREATS FIRST

Imagine a data breach or other form of attack compromising some or all of a company's records as a coffee stain spilling on some or all of a company's white shirt.

If this business wanted to wash their shirt to remove the stains—or in other words restore their breached information—they wouldn't start furiously scrubbing the stains if there was still a chance coffee could spill on the shirt.

Similarly when it comes to security breaches of any shape, size, and source, the first step a business must take is not to immediately start responding to the single attack, but to instead take the preventative steps to ensure the cause of the breach has been fully removed—

thereby stopping damage where it started without another attack occurring.

EMPHASIZE THE IMPORTANCE OF INTERNAL COMMUNICATIONS

While a company IT department or other securities managers may receive more than their fill of media attention following an attack, other officials or departments like PR will likely be the ones handling public response—making communications between these two departments or other related parties essential.

Miscommunications and changing facts hurt the reliability of a business already under the gun in the public eye. In order to ensure a professional and presentable image in the face of disaster, businesses must be sure all employees from top to bottom are informed and up-to-date so attacks are handled properly.

MANAGE PUBLIC RELATIONS – RESTORE EXTERNAL TRUST

Besides the expenses required to mend the immediate damage caused by business identity theft and data breaches, another more-subtle cost of these attacks is the damage done to reliability and trustworthiness of the victim company.

Many customers will be worried of their information potentially being stolen again in the future, or at the other end of the spectrum, some others may worry about companies trying to minimize their portrayal of the damage and stolen information to help save face.

As a result, companies are now strongly encouraged to be as forthcoming and open as possible when communicating with the public, as it helps to portray reliability and a proactive approach to resolving problems.

During communications with the public, a business should try to emphasize an image of transparency and sincerity as they provide support for affected parties. Additionally, focus on plans for improvement, as rebuilding and improving now helps to restore trust that a similar attack can be prevented in the future.

PRACTICE, LEARN, AND OPTIMIZE RECOVERY PLANS

In a constantly-changing security landscape for businesses, it’s important to constantly be looking for places to improve company response plans, as attackers are always improving their methods.

Whether your business has been recently attacked, or another separate company has just had its own time in the spotlight during the midst of a breach, take the contributing factors and other causes leading up to these incidents as the data and research needed to create a successful data breach recovery plan for the future.

This way, businesses are always prepared for the worst of *today’s* threats—rather than what has shaken the business world to its foundations in the past.

CONCLUSION – CLOSING THOUGHTS TO KEEP IN MIND

Although like any other type of crime, data breaches and commercial identity theft have no foolproof method of prevention, there are certainly plenty of preventative measures available to companies to help reduce the chances of an attack by as much as possible.

Above all, the key is in proper long-term planning—including a particular focus on aspects of the business such as how records and information will be stored, secured, and of course, an emergency breach recovery plan for how the company would respond in the face of disaster.

So as you now either take the initial steps to create a draft for document management and breach recovery plans, or are working to actively revise and improve existing processes, be sure to keep these final considerations in mind:

- **Evaluate Record Storage and Management Needs –** Before businesses can plan to prevent and recover from information being compromised, they need to know how it will be stored and facilitated. The choice to manage records using a DMS, cloud storage system, or even via offsite facilities will impact not just how security is managed, but who will need to be involved in the management process.

- **Keep a Constant Eye on the News –** From the latest in recent legislation regarding handling data breaches and information security, to company data breaches or modern types of attacks, staying up-to-date on what's going on in the world around your business is essential if you want to avoid being just another victim.

ADDITIONAL RESOURCES

Data Breaches Aren't Going Anywhere—A Growing Trend

As the overall frequency and severity of data breaches rises, the question for businesses large and small now becomes what are you doing to prepare? Learn more about the recent growth of data breaches and the development of new types of attacks to get an idea of how best to protect your company with this in-depth white paper.

Best Practices in Business: Protecting from Electronic Threats

While modern business has updated its data management and record storage strategies to boost efficiency and productivity in the workplace, hackers, identity thieves, and other attackers are also updating their tactics to prey on their victims. Get an in-depth breakdown of the modern threats companies must prepare for, as well as some top protection strategies here.

How Data Breaches Affect Small Business

Although major data breaches affecting hundreds of thousands of individuals receive the majority of media attention, small businesses must deal with their fair share of data breaches also. Learn more about the specific risks threaten small-scale business today, as well as top solutions for securely storing information so you can avoid being just another victim.