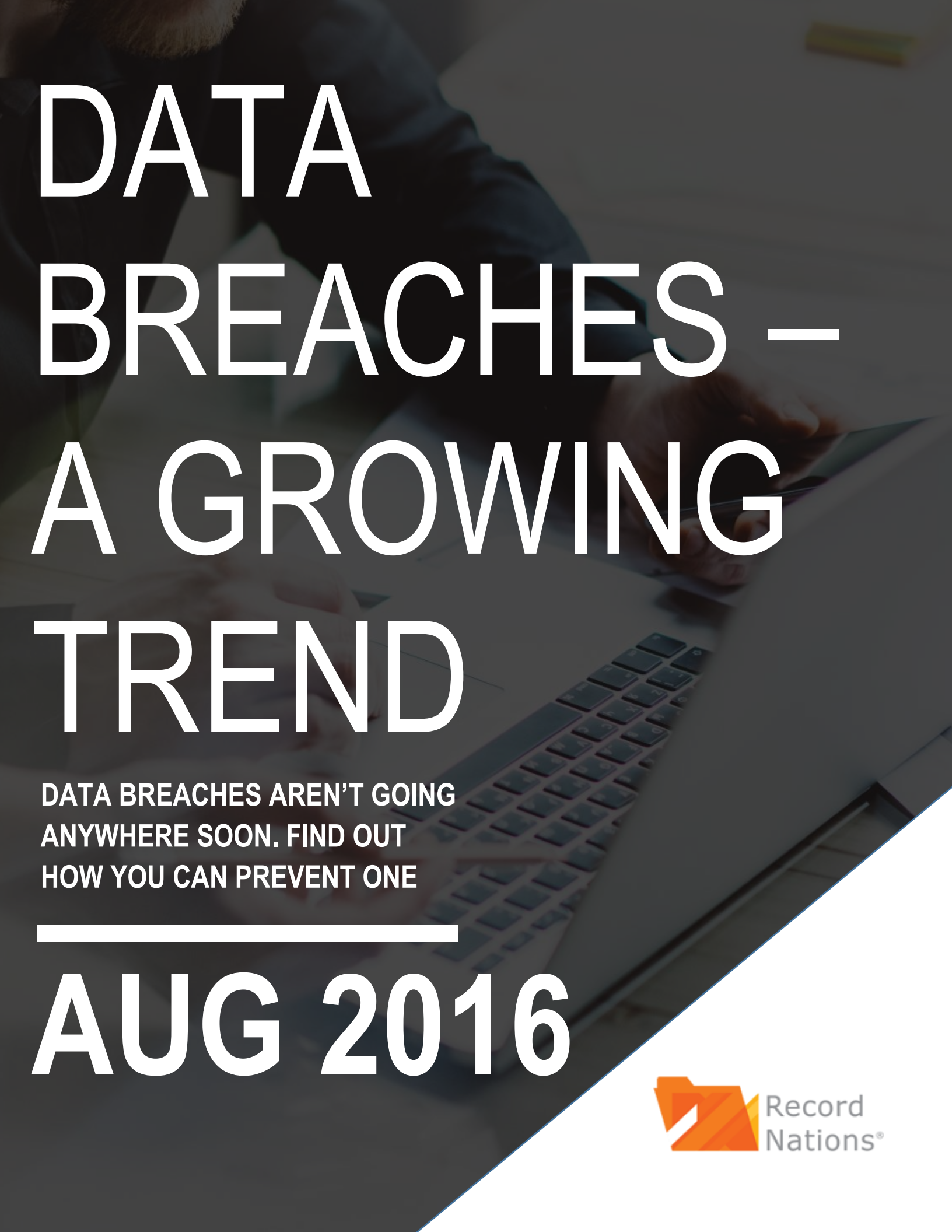


DATA BREACHES – A GROWING TREND

DATA BREACHES AREN'T GOING ANYWHERE SOON. FIND OUT HOW YOU CAN PREVENT ONE

AUG 2016

Record Nations®

777 S WADSWORTH BLVD 3-250
LAKEWOOD, CO 80226

RECORDNATIONS.COM

INTRODUCTION

BY RYAN MCHUGH

At the turn of the 21st century, you were more likely to hear talk among friends or colleagues about Y2K than a data breach leading to hundreds of thousands of customers' credit card information being released online. In fact, most people would have likely called you crazy if you tried to tell them that one day it would actually happen.

But when Black Friday rolled around in 2013, all of that changed. Skyrocketing the term "data breach" into the public eye, discount retailer Target suffered a crippling breach spanning the course of multiple weeks that, by its end, affected roughly 40 million customers and left the massive company scrambling.

While Target was not the first to suffer such a fate—and certainly won't be the last—they were among the first major corporations to be breached. When you consider for a moment the security capabilities of a large company versus a small business down the street, one can quickly begin to see the significance in companies like Target, Home Depot, and others suffering data breaches.

Rather than burying one's head in the sand, the rising trend of data breaches is a reality that all people must accept, which is why regardless of who you are—be it a business owner or an individual—you must be sure to take the proactive approach when protecting yourself from the threat of a data breach.

Throughout this in-depth white-paper, we take a closer look at the growing trend of data breaches over the past decade—breaking down not just their types and causes to help you understand the threats at hand, but also a variety of strategies and services for users of both electronic as well as hard-copy documents to take when combating data breaches.

DATA BREACHES ON THE RISE

Involving both unintentional and intentional releases of secure information to an untrusted environment, a data breach is a security incident in which this confidential information is copied, transmitted, stolen, or otherwise misused by an unauthorized party.

A growing concern for company executives and individuals alike, both the cost as well as overall volume of data breaches has continued to increase year over year for the past decade.

With causes of recent breaches alone able to be tracked back to countless sources, incidents can range from malware or other electronic attacks to careless disposal of computer equipment or paper documents. The possibility of intrusion can even arise if credentials to your network are stolen from a third-party vendor you worked with in the past.

Today, it is imperative that business leaders understand the scale and impact of data breaches on not just the internet security industry or any other single industry for that matter. Rather, the increasing threat of data breaches is one that leaders across *all* industries must face.

To put the presence of data breaches in perspective, the Ponemon Institute conducts an annual, IBM-sponsored "Cost of a Data Breach Study", and in the latest study, determined based on previous research that one in four businesses would experience a data breach of 10,000 or more records during 2016.

So now the question becomes: how will you protect yourself? With causes for data breaches coming from all directions, it can seem as if your information is exposed anywhere you turn.

In order to prevent the possibility of a data breach occurring and to best protect both yourself and your sensitive records—whether they're electronic or hard-copy—the first step to take is truly shoring up on your knowledge since, after all, it is power.

With the ability to first understand the threats at hand, companies can then take preventative measures towards upping their securities and avoiding the chance of being just another statistic in the growing rate of data breaches today.

"In order to prevent the possibility of a data breach occurring and to best protect both yourself and your sensitive records—whether they're electronic or hard-copy—the first step to take is truly shoring up on your knowledge since, after all, it is power.

HOW HACKERS GET AHOLD OF ELECTRONIC INFORMATION

From nightly news stories to tech blogs and interviews with internet security specialists, terms like malware, hacking, and encryption seem to come up time and again when major data breaches like the 2013 Target data breach occur. No matter how large and seemingly powerful companies like Target may seem—none are invulnerable to the threat of a data breach occurring. With the average cost of a data breach at $0.58 per record lost, a data breach can shake even a small business missing several thousand documents to its foundations—let alone a massive corporation losing possibly millions.

Today an increasing number of individuals as well as companies are using digital technologies to store their personal and business information. Given this growing trend, it is also becoming more necessary for organizations to familiarize themselves with the different types of electronic threats and attacks in order to best defend themselves.

Here are the top 5 most common electronic attack patterns for businesses in recent years:

28.5% POINT OF SALE

At any cash register, gas pump, or even internet shopping checkout page, a business's point-of-sale system is placed wherever its sales or transactions take place. When a customer hands over their credit card or other form of purchase information, this data can be captured by a hacked point-of-sale system, and used fraudulently elsewhere.

When Target and its customers were sent into a panic during the holiday season of 2013, attackers uploaded malicious software designed to target customer credit card information to the company's point-of-sale systems after gaining unauthorized access to the company network via a hired third-party vendor.

During the data breach, Target announced that the information of approximately 40 million customers paying for their goods at registers in their stores was stolen—certainly making up a large percentage of the contributions point-of-sale incidents make to the growing number of data breaches each year.

18.8% CRIMEWARE

When referring to crimeware, this may be closer to what one might immediately imagine upon hearing "electronic attacks". Crimeware can be various types of malicious softwares that—regardless of their design specifics—are made to facilitate illegal online activities and fraudulently obtain either informational or financial gain.

Ranging from spyware and malware made to gain access to your system and track your activity on your computer, to keyloggers able to record your keystrokes (and in turn, your passwords), crimeware comes in all shapes and sizes—and can come from all places as well.

Often, victims of crimeware attacks will have their electronic records and documents compromised without ever knowing about it—making knowledge and proper preparation the best defense for preventing a data breach caused by crimeware.

18% CYBER ESPIONAGE

Similar to what crimeware attackers may hope to accomplish, cyber espionage involves compromising network securities in order to gain unauthorized access to sensitive or proprietary information—typically belonging to a government or rival organization.

Cyber espionage attacks can be traced back to many sources, including abuse of employee access privileges (where they may either sell this information, or take it to a

rival company), or even a malware or other crimeware-based attack.

However, as with any form of electronic attack that has the potential to cause a data breach, taking steps such as encrypting your records and securely managing them using cloud storage services or an electronic document management system (DMS) is certainly a step in the right direction for preventing an attack.

10.6% PRIVILEGE MISUSE

According to a report by the Association of Certified Fraud Examiners (ACFE), the average company loses 5% of its annual revenue to fraud committed by its own employees.

Of those employees who abuse their privileges and access to confidential or proprietary records, most incidents are caused by trusted employees in executive, accounting, sales, operations, customer service, or purchasing positions.

To best counter this threat—which can be difficult to effectively manage while still assuming innocence until proven guilty—the best option is to limit and keep up-to-date on your employees' access to sensitive documents so that only those who absolutely need access have the authority.

9.4% WEB APPLIACTION

People use the internet with increasing frequency—from online shopping, to finding their way around, and even placing food orders—and with that, the frequency of web application development has grown also.

Websites like Facebook and Amazon store the login credentials and saved payment information of their users in vast online databases, which are kept on servers. In order to protect these servers from attackers, they are often protected with firewalls or other various securities. However, this still leaves the application layer—or the places where users can enter information into the site—exposed to the outside world.

This application layer is where most web application vulnerabilities are found and where attacks occur. Relying on complex user-input scenarios, the attacker can manipulate application input and exploit security misconfigurations or other application vulnerabilities in the site.


Compliance

HOW HARD-COPY DATA BREACHES HAPPEN

Although it can be easy to draw the quick connection between the phrase “data breach” and modern terms like computers, hackers, malware, and other online threats, data breaches can come in all shapes and sizes—including taking on the form of a hard-copy data breach.

Besides just taking on different shapes—and in this case, different document formats—the *causes* of a hard-copy data breach can come in multiple forms as well. In 2015, for instance, there were three primary contributors to data breaches of paper documents: malicious or criminal attacks, system glitches or losses, and human error.

LOST AND STOLEN HARD-COPY RECORDS

Hard-copy documents can be lost and stolen in a few different types of situations. In some cases, access privileges can be abused by an employee, leading to countless records being stolen and a data breach occurring from internal causes.

At the same time, however, businesses should also not discount simply losing their records as a potential cause for a hard-copy data breach. Massive companies that manage hundreds of thousands of documents can quickly begin to accumulate duplicate and out-of-date copies of records.

Because of this oversized document inventory, some companies may end up devoting entire offices just to storing their records.

The danger in this, however, is that it exposes this centralized collection of documents to being destroyed in one fell-swoop. All it might take is a single disaster to do irreversible damage to decades of company files.

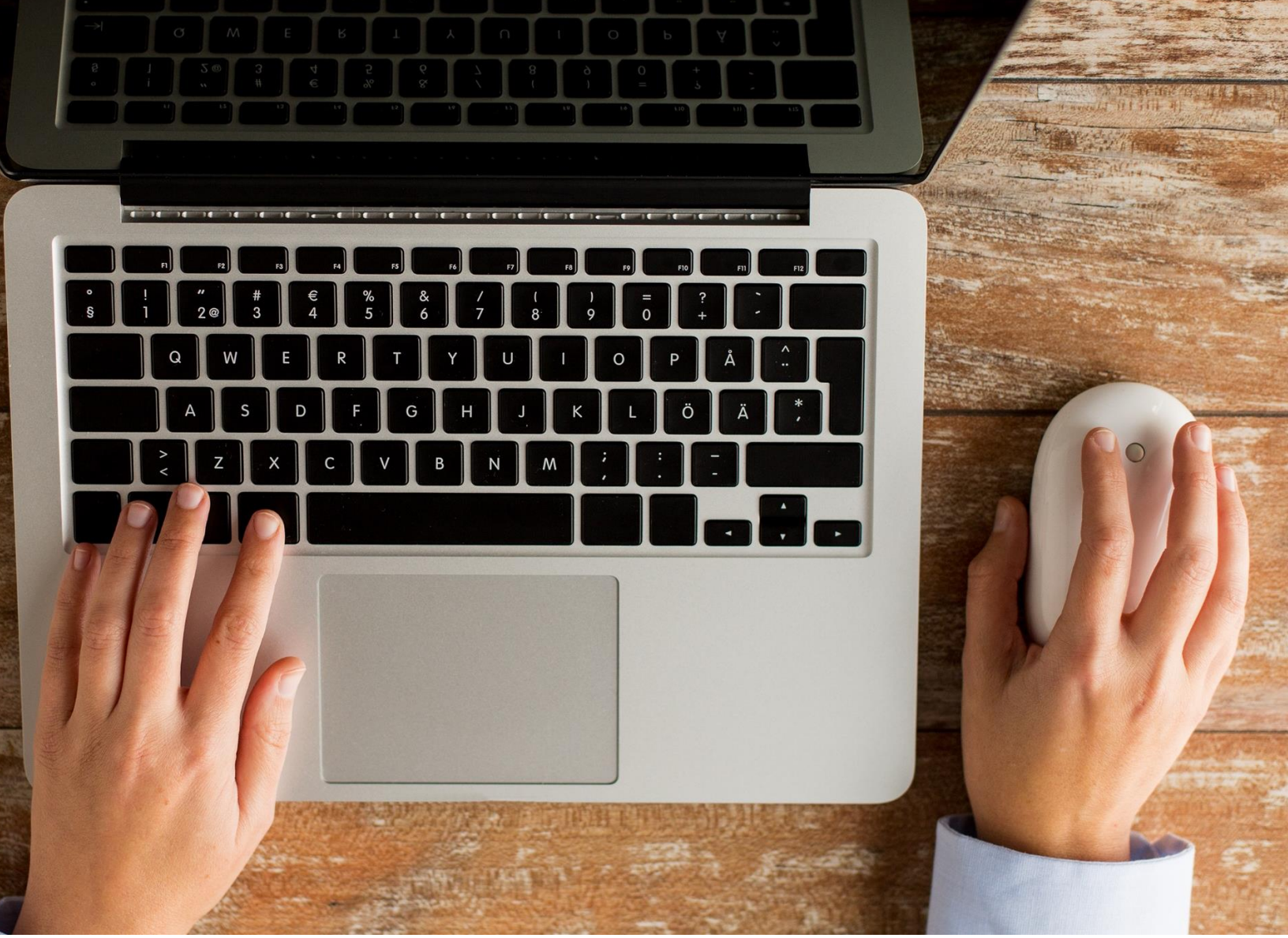
IMPROPER DOCUMENT DISPOSAL

While lost or stolen documents are certainly nothing to bat an eye at, the causes for these types of data breaches are often out of the control of the victim company.

On the other hand, hard-copy record breaches caused by improper document disposal leave no one for these businesses to point the finger at other than themselves.

In many cases, businesses who improperly dispose of their documents do so unintentionally—usually tossing documents containing either private information of customers or the proprietary information of their own company in public dumpsters or other easily accessible places.

Although accidents do happen—it doesn’t lessen the financial impact of a data breach caused by leaving sensitive documents entirely exposed to dumpster-divers and other nefarious individuals.



TOP DATA BREACH PREVENTION STRATEGIES

Among other initial steps in protecting against the threat of a data breach shaking an organization to its financial foundations, creating and outlining a comprehensive document management plan that details the document process from creation to destruction is a good way to begin staying on top of your records. There are typically eight essential components to include in every document management plan:

1. **Conduct a complete inventory of all your existing records**
2. **Determine who will be responsible for your record management process**
3. **Develop a record retention and destruction schedule**
4. **Evaluate and determine the best methods for storing and managing your records**
5. **Create and document proper company policies and procedures**
6. **Create a disaster recovery plan in case of data breach or other emergencies**
7. **Implement your document management plan and train employees**
8. **Maintain and audit your program for efficiency and effectiveness**

Although creating a document management plan is an ideal place to start for helping your company to prevent the threat of data breaches, there are also more specific tactics that companies using either electronic records or hard-copy documents can take to provide themselves additional protection.

ELECTRONIC RECORDS

ENCRYPTION

By modern standards, encryption is a powerful technology used internally by businesses to protect confidential records. Dating back long before the introduction of computers and digital technologies to everyday business, cultures as old as the ancient Egyptians have used encryption to secure sensitive information and messages.

Today, however, one of the most important steps companies can take towards protecting themselves from the threat of a data breach is to ensure that they encrypt all their information.

Although some laws have mandated encryption requirements for specific industries, a large percentage of companies continue to take the risk of going without, leaving their sensitive information exposed and waiting to be breached.

CLOUD STORAGE SERVICES

Besides just encrypting and protecting electronic data, it's also important that businesses consider how they will store their records. When it comes to electronic files, there are typically two primary management options—cloud storage systems and electronic document management systems.

With cloud storage services, these systems are usually hosted in an offsite data center. Offering the additional convenience of being able to access your documents from anywhere at any time while using a computer, tablet, or mobile device, the best part is that many cloud storage service providers include technologies like SSL data encryption as part of your leasing fees.

ELECTRONIC DOCUMENT MANAGEMENT SYSTEM (EDMS)

An alternative to cloud storage, faster-performing electronic document management systems (DMS) are also available for managing electronic records. While cloud storage is hosted and managed offsite, DMS services require in-house management. While electronic document management systems may not be ideal for a business that is less technically-savvy or doesn't have an internal IT department, one of the greatest advantages to using a DMS is that these systems offer extensive room for customizations including firewalls and encryption.

HARD-COPY DOCUMENTS

Some companies deal with information and records—such as legal documents—that are required to be retained in their hard-copy formats. If this is the case for your business also, then investing in offsite record management and storage facilities could be an ideal solution.

Offsite storage services for paper documents not only help to limit access—potentially preventing a disgruntled employee from abusing their access privileges to sensitive information—they can also help to provide protection from environmental hazards like fire, as these facilities are climate-controlled. Another option for companies who have a large inventory of hard-copy files but are interested in alternative storage methods is scanning and converting these documents to electronic formats.

When there are thousands of company records needing tracking, the process can be greatly streamlined if done electronically. Not only can documents be stored, sorted, and sifted through more simply—they can also be protected and more easily safeguarded from risks that threaten hard-copy records like misplacement or improper disposal.

CONCLUSION – FINAL CONSIDERATIONS TO KEEP IN MIND

So, after having a full understanding of the growing role data breaches play in both electronic and hard-copy information security, now comes the time to bring the question full circle—how will you manage the risk?

You needn't worry about being paralyzed with indecision—there are multiple options and routes for businesses to take depending on the individual goals and means available to your organization.

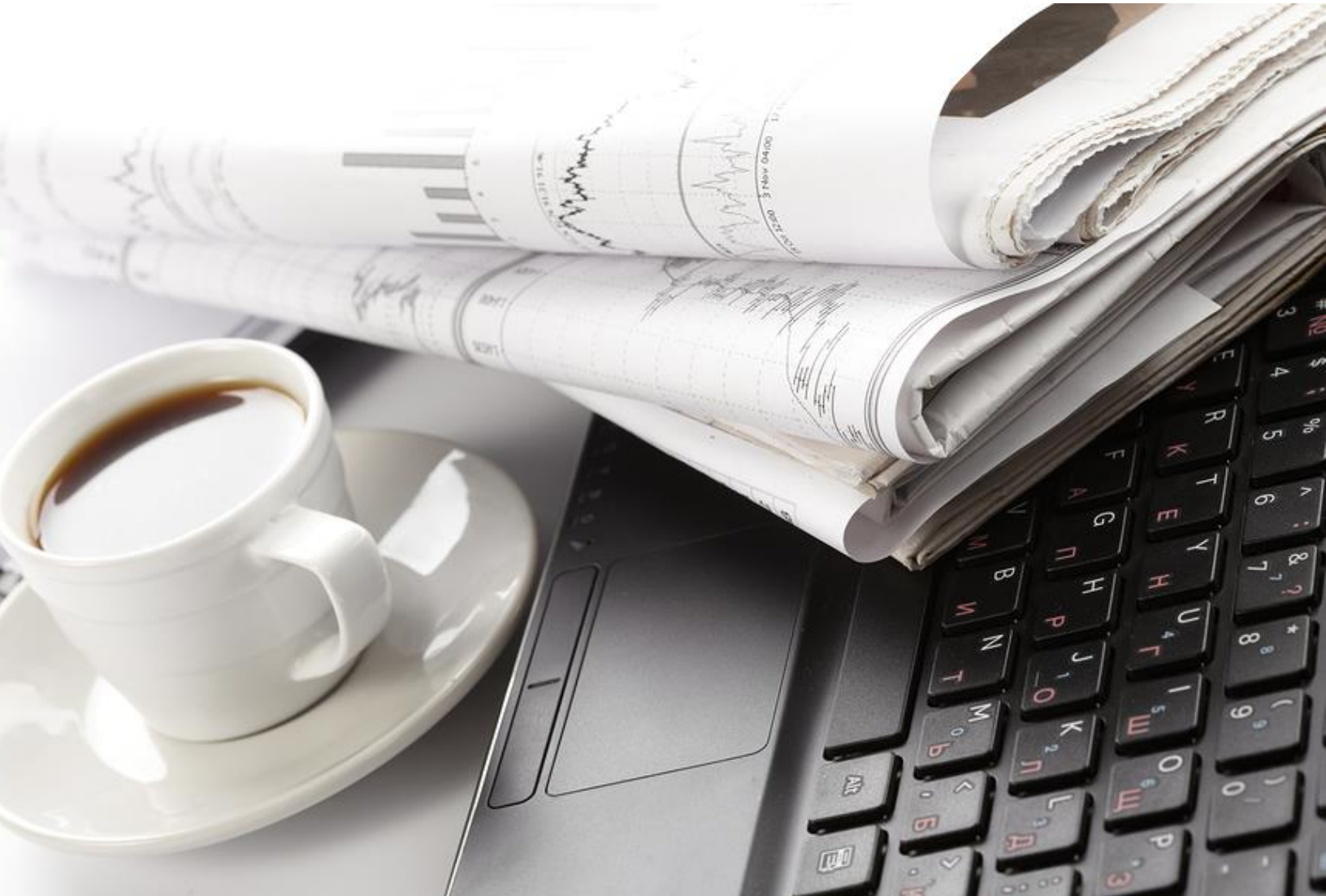
Here are a few final guidelines and best practices to keep in mind for minimizing the threat of data breaches:

How Will You Manage and Store Your Sensitive Documents?

When you initially consider how you will address the storage and management of your company records, first consider the needs of your business. Do you require hard-copy storage? If so, then offsite record facilities may suit your tastes. Otherwise, think about cloud storage or a DMS if you have the IT to support it.

Account for Data Breach Contributors

Whether you favor electronic or hard-copy records—or even a combination of both—it's essential you account for the various factors that contribute to data breaches. From ensuring that your access privileges are limited to only those who need it, to either outsourcing security needs or managing them in-house, make sure all bases are covered.



ADDITIONAL RESOURCES

Best Practices in Business: Protecting from Electronic Threats

A growing number of businesses and individuals alike are continuing to transition towards digital documents and data—leaving identity thieves and other criminals hurrying to update their tactics. In this in-depth white paper, we explore the process of protecting information from electronic threats, covering not just the risks to look out for, but also the best protection strategies as well.

The Most Vulnerable Spots for a Data Breach

With the Target data breach serving as just one example out of many, it's important that businesses are aware of the gaps they may have in their security fences. Here, we take a closer look at some of the greatest weaknesses in the modern company's securities and how they can lead to a catastrophic data breach.

Ransomware: One More Reason to Encrypt Your Records & EDMS

Besides just the growing trend of data breaches themselves, there is also a more specific breach epidemic—otherwise known as ransomware—plaguing industries today. In this article, we provide a breakdown of just what exactly ransomware is, and more importantly, offer businesses a variety of electronic strategies for protecting their information.