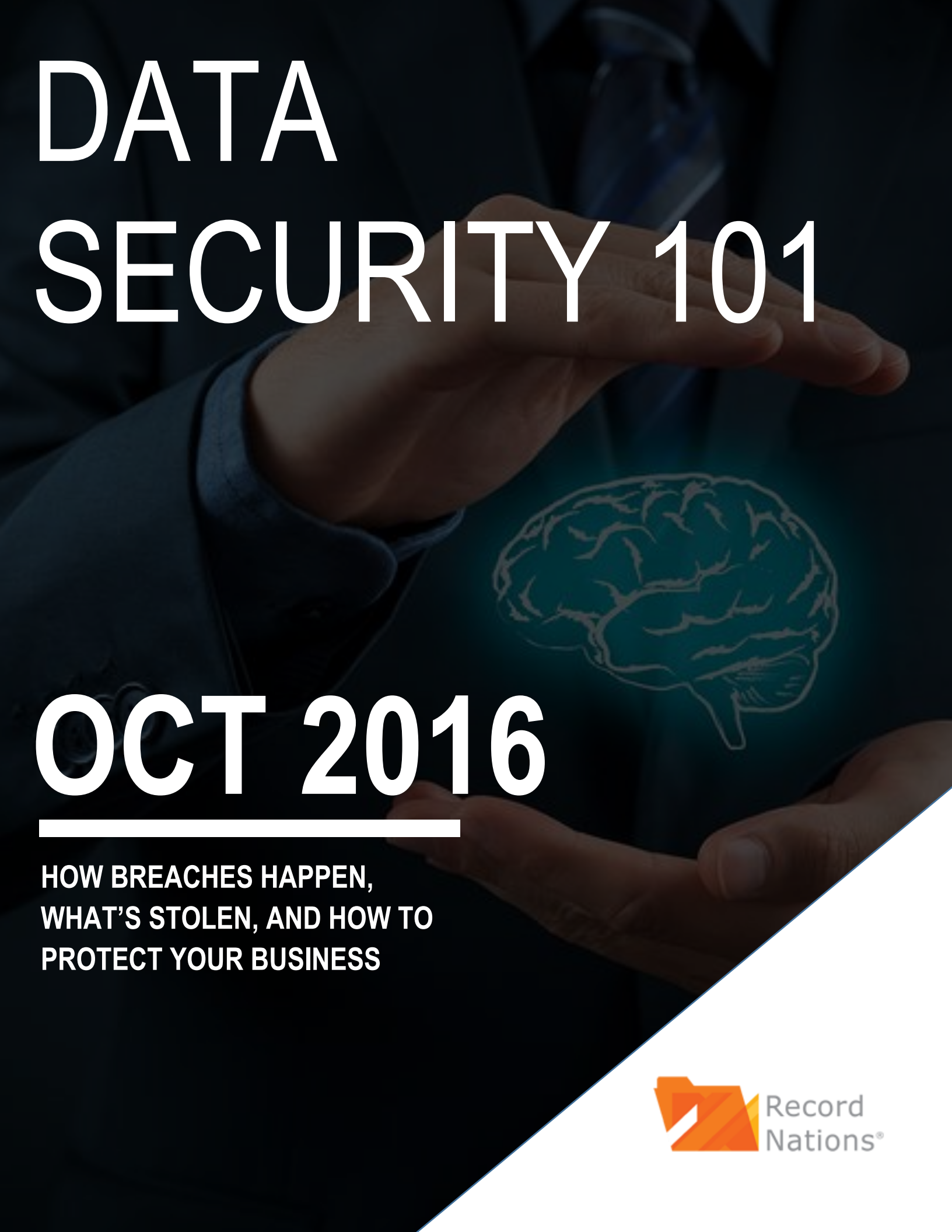


DATA SECURITY 101

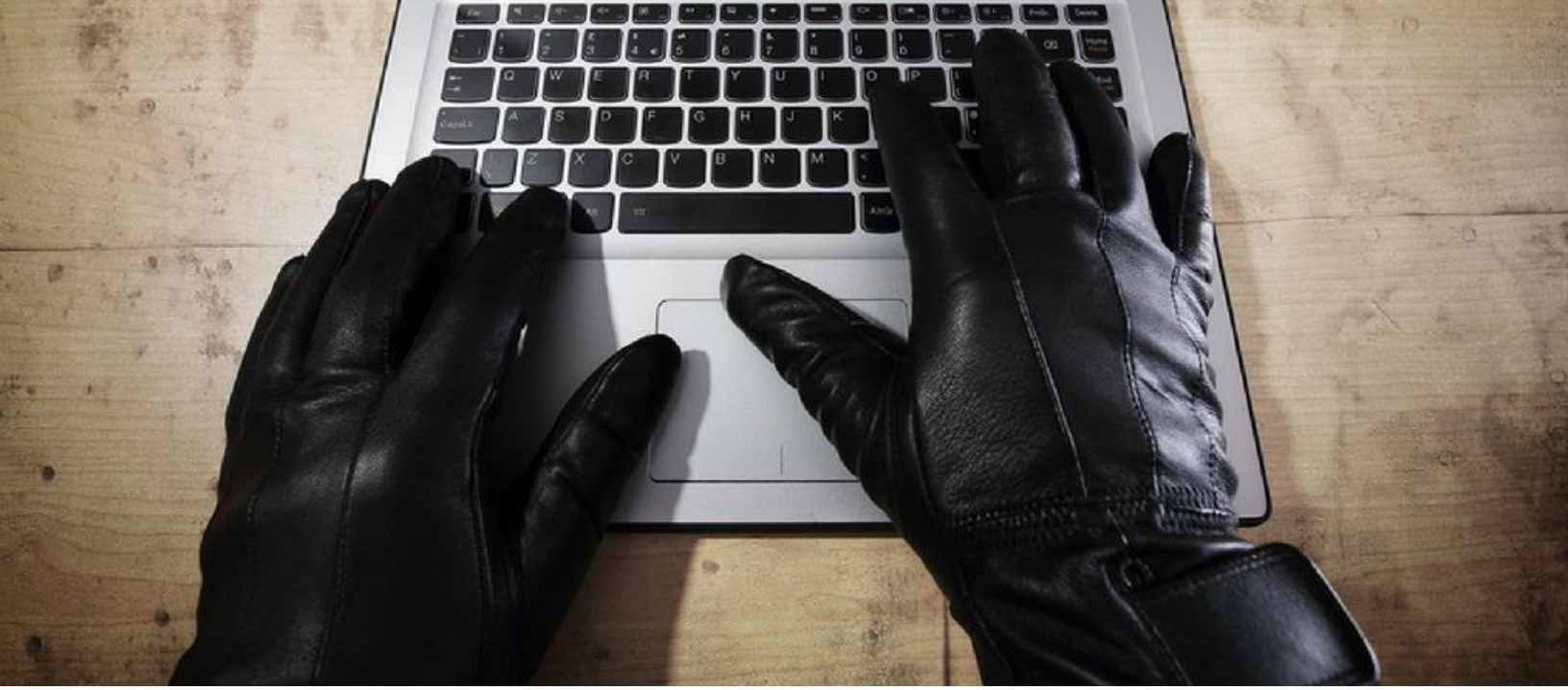
OCT 2016

HOW BREACHES HAPPEN, WHAT'S STOLEN, AND HOW TO PROTECT YOUR BUSINESS

Record Nations®

777 S WADSWORTH BLVD 3-250
LAKEWOOD, CO 80226

RECORDNATIONS.COM



DATA BREACHES TODAY – TURNING THE SECURITY LANDSCAPE UPSIDE DOWN

BY RYAN MCHUGH

By now, the term "data breach" and the accompanying threats of data theft, hacking, and other malicious digital activity have rudely forced their way center-stage into the mainstream of the business world, placing an even greater priority on the security of information.

With news stories cropping up seemingly each day detailing incidents ranging from sensitive government emails being exposed to millions of user accounts or customer information being stolen, many companies may now be asking themselves what they can do to ensure they avoid similar disasters.

Requiring businesses to take a harder look than ever at their processes for managing sensitive electronic data and ensuring it is securely stored, the growing presence and potential threats both data breaches and theft pose to business leaves attention to information security all the more essential to preventing a breach.

Whether for purposes of managing document version and access control, better organizing massive document inventories and streamlining daily operations, or taking advantage of potential securities like encryption, a growing number of companies today are adopting electronic document management systems or cloud storage services.

However, with this transition to newer and more advanced electronic systems for managing documents and data, the opportunities for businesses to have information stolen or compromised by hackers, insiders, or even by accident are also shifting.

Consequently, if companies are planning to protect their information from these risks, there is now a need to stay a step-ahead of new issues. With security experts now urging businesses to approach data breach planning, prevention, and response from the perspective of not *if,* but *when*, it's essential for companies to understand current risks and strategies for protection.

Throughout this white paper, we take a closer look at the modern world of digital information security—providing an in-depth breakdown of not only the top causes of recent data theft and breach incidents, but also real-world examples of other company's approaches to data security and what businesses can learn from them to prevent a data disaster of their own.

DATA THEFT AND BREACHES IN THE NEWS: A CLOSER LOOK

It can seem as if there's a major data breach reported every week. In fact, this may be partially true—in just July of 2014, approximately 30 breach incidents in the healthcare industry alone were added to the still-growing list of breaches today.

Companies of all shapes, sizes, and industries have been making the news with stories of their sensitive documents and data being compromised—and while it may seem no one is safe to the casual onlooker, there is plenty a business can do to protect itself from a similar fate.

Beginning with understanding the problems from top-to-bottom and recognizing where companies in the past have made the right and wrong decisions, future companies can learn from the previous mistakes of others to better evaluate their own security priorities and needs.

The following is a brief case study comparing the differences between the right and wrong ways to protect from a breach—as well as their potential impacts:

DON'T MAKE THE SAME MISTAKE – ANTHEM 2015

Serving as an ominous example to other companies, in February 2015 the health plan provider Anthem Inc. reported a record-breaking data breach affecting just under 80 million individuals.

Following further investigations, it was discovered that the source of the breach stemmed from the credentials of five IT employees had likely been stolen through a phishing attack.

Although phishing attacks are a common tactic for data thieves targeting businesses and individuals alike, the potential impact to companies is much greater, as several major data breaches in recent years alone have been tied to phishing attacks.

Consequently, it is essential that companies take a more aggressive approach to educating their employees on not just proper data management and storage practices, but also how to recognize common threats and protect sensitive information from them.

Despite this however, many security experts may still ask how accessing the accounts of five employees could lead to 80 million records being stolen, as the sheer volume of

information compromised suggests security and accessibility issues that cannot be addressed by simply educating a workforce.

Besides educating employees, companies can—and should—take additional steps to avoid a fate similar to Anthem's by instituting a "minimum necessary" policy for managing company information and data.

By restricting access to sensitive information to include only individuals and users who explicitly need it, the potential damage and impact of a breach can be vastly minimized should company information ever be compromised.

SETTING THE STANDARD – SECURITY PRACTICES TO FOLLOW

On the flip-side of past blunders made by other companies, organizations like Boston's Beth Israel Deaconess Medical Center are able to provide a better example of security practices and policies for companies to follow when working to shore-up on company data protections.

As the CIO, John Halamaka, stresses with Beth Israel Deaconess' own security policies, some of the greatest risks for data breaches today stem from internal sources—making it all the more critical their internal security policies are clearly established and rigidly enforced.

In the past, organizations usually made efforts to hide or downplay data theft and breaches. Today however, there are changing perspectives on data breach response, as many experts now place greater emphasis on clear communication between companies and the public to better preserve a trustworthy image for the company in the public eye.

While many businesses similarly hid or downplayed employee policy infractions and consequential terminations in the past, like changing views on data breach response, best practices for handling security policy infractions are shifting as well.

With changing regulations on data security, privacy, and data breach response for businesses, laws like HIPAA or the California Security Breach Act are now making a more transparent approach to information security the expectation.

As a result, to remain compliant with breach disclosure laws and other regulations, organizations like Beth Israel Deaconess are working to improve the standard by proactively establishing strong security policies and clear enforcement expectations for violations, rather than covering-up past breaches and other incidents.

HOW DATA THEFT HAPPENS, AND HOW BUSINESSES CAN PREVENT IT

While initial stories of data breaches gripped headlines for weeks, the number of breaches has continued to steadily rise, leaving both consumers and businesses alike desensitized with each new report. Typically a story or announcement will crop up about a company's systems being breached, and what they are doing in the immediate term to help customers.

But how often do these stories delve deeper, looking at the causes of the theft or breach—and more importantly, how other businesses can take steps to avoid similar incidents?

Not only are there more data breaches today—there are also alternative strategies attackers are adopting for targeting business information, as well as other potential risks from inside threats or even business associates for organizations to now account for.

The following provides an outline of some of the most common causes for data thefts and breaches, as well as tactics companies can take to protect themselves, including:

LACK OF DATA ENCRYPTION

With a growing number of company documents and data now being stored in electronic formats today, the potential damage

and impact of these files being exposed by various causes can also pose a threat to businesses.

As just one example, due to the large volume of information healthcare providers must keep on their patients and the value this number of records holds to potential identity thieves or other malicious individuals, healthcare is often targeted by attacks. In 2016, more than 60 hacking attacks rocked the industry—affecting nearly 11 million individuals.

While those numbers may be jaw-dropping to some, exploring many incidents in both healthcare and other industries has revealed even more alarming facts—including the number of companies who could have prevented these catastrophic data thefts and breaches by proactively addressing common security vulnerabilities.

As technology advances towards all-electronic systems for storing information, businesses are following suit, but with this transition, this also means companies need to step up their accompanying digital protections—which is where the security disconnect eventually leading to data theft or breach typically occurs.

For instance, a common cause for thefts and breaches of sensitive data is the result of companies not taking the time to ensure their information and systems are securely encrypted. By encrypting documents and data, businesses can use password protection to ensure records' contents are protected from unauthorized access.

Without this protection, companies leave themselves greatly exposed. From accidentally misplacing a flash drive or laptop, to opening a bad email and having systems crippled by ransomware, the opportunities for crimeware and other malicious activity will place an even larger target on unsecured networks and information.

To counter these potential vulnerabilities, companies are urged to evaluate or reevaluate their systems and processes for storing data and documents.

With custom-built electronic document management systems (DMS) managed by internal IT teams for example, companies can implement their own complex encryption systems. Similarly, many cloud storage services will typically also include SSL or similar encryption systems with their services.

Either way, companies can help to make certain their basic security bases are covered when they ensure their digital data and documents stored on a DMS or cloud storage system are encrypted.

EMPLOYEE NEGLIGENCE, PRIVILEGE MISUSE, OR ACCIDENTAL DISCLOSURE

Besides the risk of an external attacker compromising a company's digital data and documents from potentially thousands of miles away, another primary threat for data theft and breaches instead lies much closer to home.

Employees who work each day in close contact with sensitive information carry great responsibility to protect this information, however the unfortunate reality remains that inside employees will inappropriately access patient, customer, or company records for reasons ranging from mere curiosity to more malicious intents.

In 2014, for instance, a former radiologist of NRAD Medical Associates used his previous access to acquire the patient records of more than 95,000 individuals without authorization, adding another company to the data breach tally.

As the number of documents and overall data stored in central locations swells with electronic systems, the value to employees who may steal this information and sell it to more malevolent individuals is also greater—however this isn't the only insider threat to account for.

Aside from incidents involving direct misuse of information, numerous data breaches have been the cause of mistakes made by employees.

In an incident several years ago, the social security numbers of nearly 4,000 military veterans were unintentionally exposed when their data was merged with an old database—resulting in benefit summary letters from the VA being sent to wrong addresses and potentially leading to thousands of **identity theft** cases.

To prevent similar incidents, many data experts recommend best practices for businesses like ensuring all documents and data is properly encrypted and stored, as well as keeping their security processes up-to-date and well-communicated as the company's employees and operations ebb and flow over time.

Additionally, since many companies and organizations have turned to adopting systems for electronic data and documents which place higher priority on security, safeguards can also be implemented to help prevent internal risks, as both DMS and cloud storage services allow options for restricting user access.

At the end of the day, regardless of whether data thefts or breaches stem from unintentional or intentional causes, the potential for data breaches to come from an internal source leaves insider threats an equally important factor for

companies to account for when considering their information security process.

BUSINESS ASSOCIATES, THIRD-PARTY VENDORS, AND CONTRACTORS

While threats directly posed to companies such as external hacking, internal misuse, or accidental employee disclosure of information may seem like an already full plate for an organization, it's important companies expand their horizons to also include consideration for the security practices of business associates.

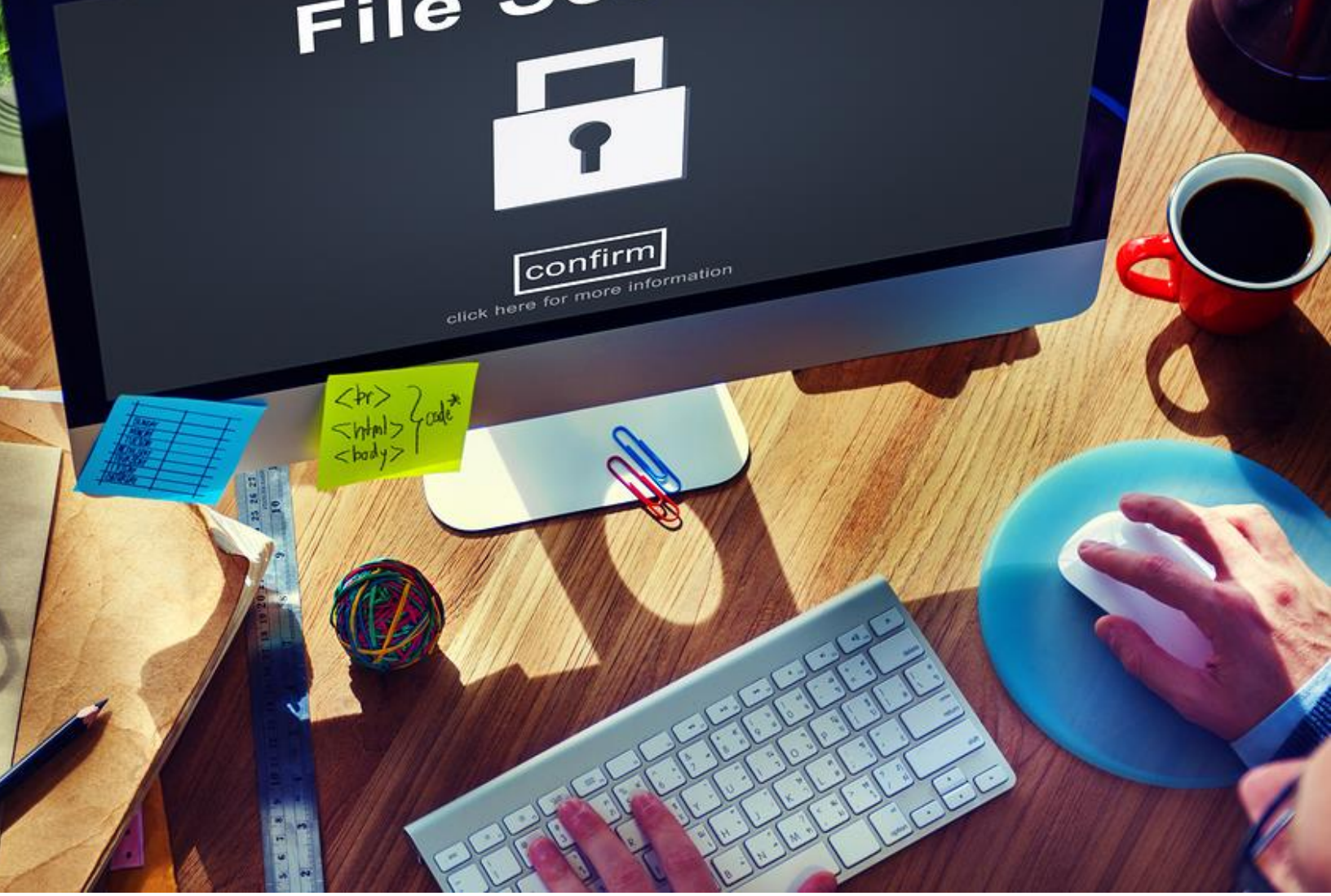
Because companies are ultimately responsible for ensuring the security of personal information for customers, companies and the business associates they work with require a codependent relationship to truly protect sensitive information.

Business associates handling a company's critical data pose a greater risk for data theft and breaches compared to other third-party vendors, and similarly, some associates may have a lower level of security maturity compared to others.

Providing a perfect example, the theft of an unencrypted laptop from the business associate of a healthcare provider several years ago serves as an ominous warning. In 2014, a laptop containing patient information of more than 68,000 individuals was stolen from the company Omnicell, a distributor of automated medication dispensing systems.

While Omnibus didn't directly treat these patients, as a business associate of the healthcare providers they worked with they required access to patient records—and despite the fact that missteps were made by the business associate, the fact still remained that the original companies were responsible for the files being exposed.

As a result, it is essential companies seriously evaluate their information security practices to not only ensure they securely store information and clearly communicate the security needs of sensitive data to employees, but to also make certain all business associates the company plans to work with are carefully evaluated as well.



CONCLUSION – FINAL CONSIDERATIONS TO KEEP IN MIND

From massive tech companies like Yahoo to smaller healthcare service providers like Omnibus, the reach of data theft and breaches extends throughout all industries.

With causes which can be traced back to sources like lack of encryption, employee negligence or misuse of information, and even a company's relationships with business associates, modern threats may seem everywhere—however with the proper preparation and safeguards implemented, a company can take steps to prevent their data being compromised.

The following are a few final considerations to keep in mind when evaluating company data security practices for potential gaps in the defenses:

What Protections Are Currently in Place? – Data thefts and breaches involving internal employee risks and the loss of unencrypted information are increasingly common. With this in mind, companies must ensure internal protections like encryption systems and company security policies are kept up-to-date to meet these security needs.

How Secure are Business Associates? – Because companies responsible for protecting the personal information and privacy of customers are also responsible for ensuring their business associates also protect this information, it's critical all third-party business relationships are carefully evaluated to prevent breaches and steep fines down the road.

ADDITIONAL RESOURCES

Planning for Business Identity Theft & Data Breaches: The Guide to Prevention

The adoption of more convenient and streamlined electronic systems for managing data has opened the modern business landscape to now include new options for how this information is stored—bringing with it new tactics for identity theft and other malicious attacks. Use this guide for an in-depth look at the new threats businesses must look out for, as well as essential aspects to be included in every company's data breach response and recovery plans.

Data Breaches On the Rise: A Growing Trend

Besides the growing rate of data breach incidents over the past decade—the overall damage and and consequential costs associated with being hit by a breach are also rising. With this white paper, we provide an in-depth outline of not only the most common contributors to data breaches, but also top data breach prevention strategies as well.

Ransomware: One More Reason to Encrypt Your Records & EDMS

While encryption today is intended to be a protective strategy for businesses by helping to keep important information out of the wrong hands, ransomware turns the tables on companies that haven't taken advantage of encrypting their information—locking these files away from their While encryption today is intended to be a protective strategy for businesses by helping to keep important information out of the wrong hands, ransomware turns the tables on companies that haven't taken advantage of encrypting their information—locking these files away from their rightful owners and forcing them to pay a ransom in exchange for decryption. Get the breakdown on ransomware in healthcare today, as well as tips on how to protect yourself here.