REDUCE YOUR REPUTATIONAL RISK:

A Guide to Help Mitigate Marketing Blindspots Associated with Customer Data Collection & Retention

ALMOST 2/3 OF COMPANIES ARE LEAVING 1,000+ RECORDS COMPLETELY OPEN

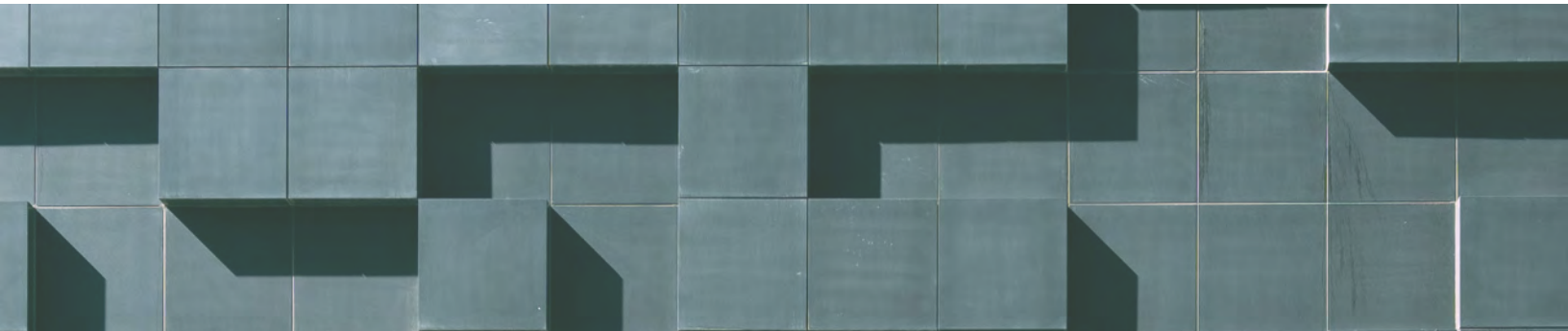


TABLE OF CONTENTS

The PII Collection Conundrum

PERSONALLY IDENTIFIABLE INFORMATION

PII Personally Identifiable Information (PII) is something that almost every business collects. Marketers rely on this data to ensure relevance for their customers, as well as tracking Key Performance Indicators (KPIs) for ongoing optimization. For large enterprise clients, managing this mass amount of incoming data can become a balancing act.

Customer-facing operations, marketing strategies, and customer care solutions typically collect personal data. Email addresses, customer names, logged IP addresses are just some of the most commonly collected pieces of information, which are all considered forms of PII and are protected under GDPR compliance laws.

Without regulation and policies to control this incoming feed of information, enterprises can quickly find themselves sitting on a horde of data.

Some of this data is useful and offers long-term value for enterprises to retain. However, a substantial portion of this data loses its value over time, and some information being collected may offer no intrinsic value for the business at all.

Without procedures in place to downsize and regulate the volume and types of data being stored, as well as security measures to protect it, a small portion of valuable data can become buried under an avalanche of unnecessary information. This adds to the potential risks associated with data breaches if/when they occur.

Planning for Problems

Data breaches are something that no company wants to face, and it's crucial that security measures (technical solutions and proactive problem-solving) are put in place to prevent data leaks wherever possible.

Regardless of the protections an enterprise already has, data breaches can still be possible. Whether resulting from a lack of security controls in place to protect certain types of data, accidentally misconfiguring a system, or any number of other issues that can leave a system open to PII leaks, the result is ultimately the same.

With digital technologies constantly evolving, it's no surprise that according to IBM, in 2021 customer PII was the most common and expensive type of data to be lost or stolen.

The average cost per lost or stolen PII record was $180 – for enterprises holding hundreds of thousands or millions of customer records, this can have a huge negative impact financially and reputationally.

DATA BREACHES, LEAKS AND EXPOSURE HAS AFFECTED OVER 53 MILLION INDIVIDUALS IN THE FIRST HALF OF 2022

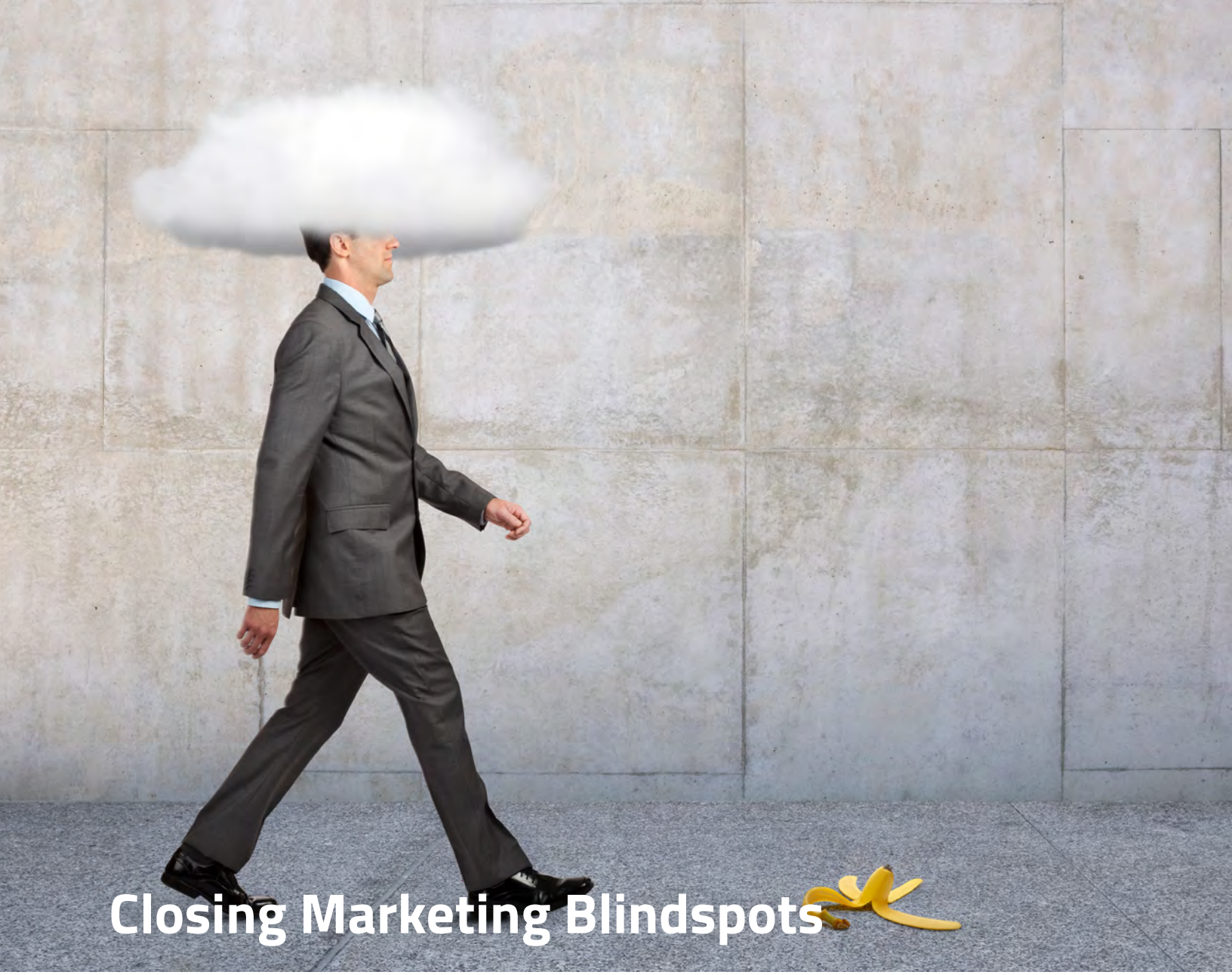
Weighing the Risks

EVERY BREACH CAN AFFECT COUNTLESS INDIVIDUALS

According to the Statista Research Department, in the first half of 2022 alone, there have been a total of 817 cases of data compromise across the United States. These breaches have affected over 53 million individuals.

If we use the same value at $180 on average per PII record leaked, this would account for roughly $9.5 billion dollars in business costs in the first half of the year alone – and that only accounts for a single record per individual.

For enterprises sitting on millions of PII records, a single leak could be financially disastrous. More than that, no enterprise wants to see their name in a headline alongside 'customer data leaks'. The reputational risk this poses to a brand's image can be devastating.



Closing Marketing Blindspots

PRODUCT SECURITY DOESN'T NECESSARILY TRANSLATE TO PII SECURITY

Security groups within enterprise companies tend to focus on protecting their internal resources – product code, IP and product system protections become the central focus for maintaining a secure network.

In many cases, this doesn't take into account all of the PII that's being collected by the marketing team through customer-facing services.

CMOs focus on growing the company's customer base and gathering information that will allow them to better engage and serve their target audience. Unfortunately, the lack of built-in protections for this incoming PII then becomes a blind spot, which can be costly if leaks occur.

DATA BREACHES, LEAKS, AND EXPOSURE HAS AFFECTED OVER 53 MILLION INDIVIDUALS IN THE FIRST HALF OF 2022

Identifying & Addressing Security Threats

HIDDEN RISKS ARE STILL RISKS

When CMOs are focusing on their marketing campaigns, it can be easy to overlook places where there is seemingly only 'limited' PII as a source of potential risk.

Although it typically doesn't involve financial or medical Personal Health Information (PHI), customer portals and online community groups are actually a significant source of PII that marketers may not be properly protecting.

As well, the 2021 Varonis Data Risk Report tells us that almost two-thirds of companies are leaving at least 1,000 or more records open to every employee, meaning they are unprotected and can be readily accessed, changed, or shared outside the organization.

And yet, the same report tells us that 70% of all sensitive data is stale. This means the data has been kept beyond the predetermined retention period. In turn, this leaves organizations exposed to higher risks and liabilities, simply because they're retaining this old data.

INCREASED INTERNAL SECURITY REQUIRES ADDITIONAL RESOURCES

It is possible to better protect data that's being stored by increasing the security systems that are in place internally within enterprise organizations. However, these additional protections can often require substantial additional resources to source, implement, and maintain.

Depending on the volume of data collected and amount being retained, this can become an expensive, time-consuming endeavor – particularly for enterprises that don't have large security teams or the resources available to easily absorb the costs of these security expansions.

ALMOST 2/3 OF COMPANIES ARE LEAVING 1,000+ RECORDS COMPLETELY OPEN.

Mitigating Risks Through PII Hygiene

MARKETERS CAN MINIMIZE POTENTIAL DAMAGE BY REDUCING UNNECESSARY DATA RETENTION

One of the most pertinent mitigation strategies that marketers can use to reduce the risk and damage of potential breaches is to downsize the amount of customer PII that's being retained.

This way, if/when a breach occurs, both the damage to the customers affected and the reputation of the trusted entity will be minimized. The 2021 Verizon Data Breach Report tells us that 60% of breaches can take weeks or longer to discover, which makes it all the more vital to take steps to reduce these potential damages before they occur.

But how can enterprises determine which data is necessary for their operations, and which data is being collected but isn't providing any value to the business?

In these cases, BKJ Digital specializes in guiding enterprises towards efficient, long-term PII hygiene practices.

The Four Steps of Data Evaluation

1

ANALYZE THE SCOPE OF CURRENTLY RETAINED DATA

Before retained data can be quantified for the purposes of reduction, it's crucial that enterprises take time to discover, identify, and analyze all the forms of PII that are currently being collected.

This process involves taking a deep look at any potential PII that's being collected through all existing customer-facing business practices. Otherwise, overlooked PII could remain vulnerable to future data breaches.

2

ASSESS THE ROLES EACH TYPE OF DATA PLAYS IN BUSINESS STRATEGIES

Each type of data may play a different role in the company's long-term business plans.

For example, email addresses may be collected for marketing purposes. IP addresses may help identify geo-specific information regarding customer and sales statistics.

If a type of PII has no value for the business, retaining the information is only adding to the enterprise's potential risks and liabilities.

70% OF ALL SENSITIVE DATA IS STALE

3

MAKE TRADEOFF DECISIONS ON DATA RISKS VS REWARDS, AS WELL AS RETENTION TIMELINES

The enterprise must spend some time evaluating the long-term value of each type of PII that is being retained to determine whether it's worth keeping and for how long.

This requires an evaluation of business utility generally, as well as business utility over time for each type of data.

If a type of PII is deemed worthy of retention, timelines need to be put into place to prevent the enterprise from continuing to retain that data after it has become stale.

4

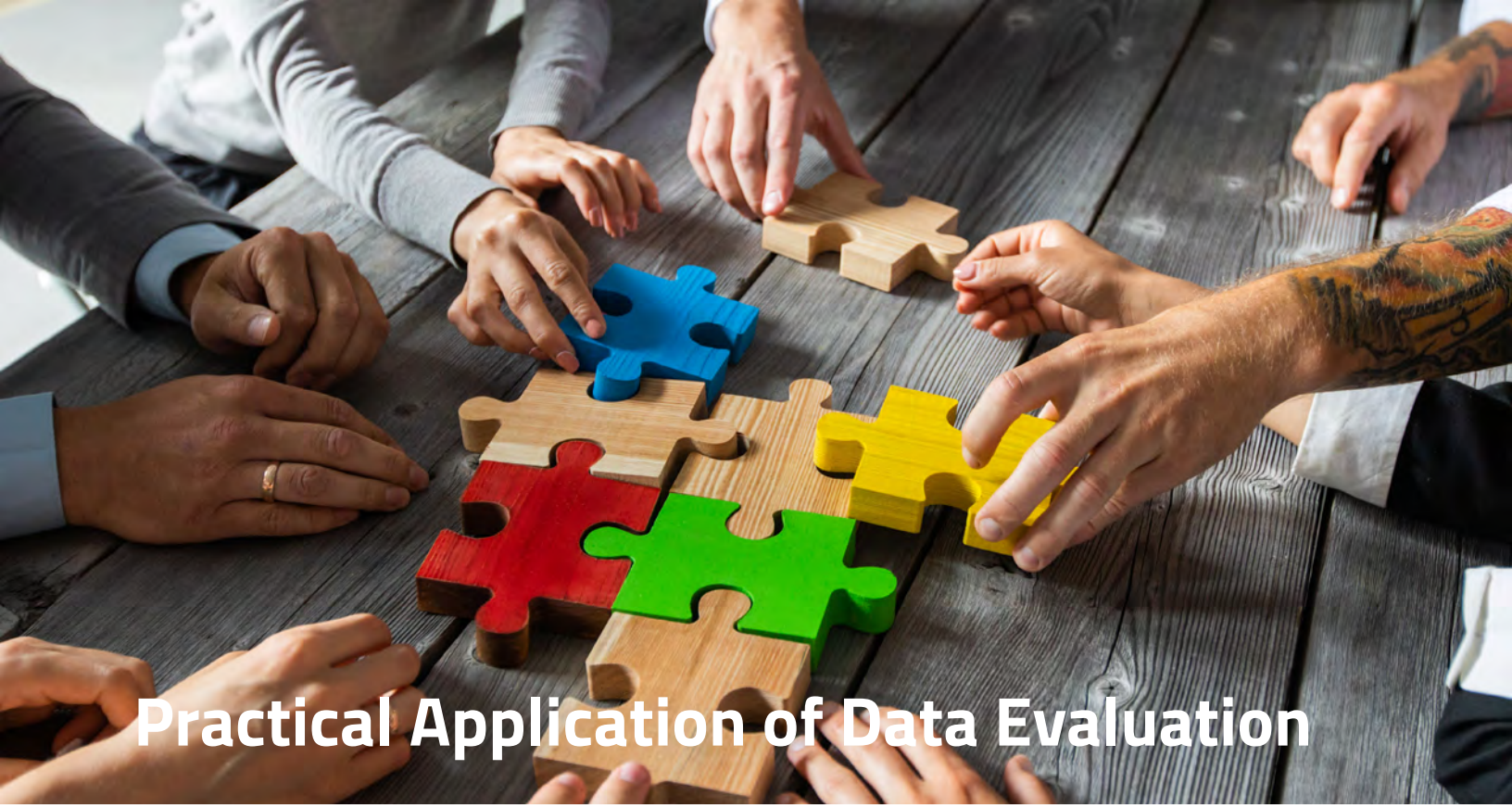
IMPLEMENT NEW PII RETENTION POLICIES AND GOVERNANCE CONTROLS

Once valuable PII has been identified and separated from unnecessary data, enterprises need to implement new policies and procedures regarding the retention and governance of future PII that's collected.

This will eliminate the overcollection of unnecessary data, and prevent the issue from occurring again down the road.

Preferably, in these situations, it's best to automate as much of this process as possible through new policies and procedures, so that less resources need to be allocated in the future to manage these needs.

60% OF BREACHES TAKE WEEKS OR LONGER TO DISCOVER



Practical Application of Data Evaluation

ENTERPRISES MAY BE COLLECTING EXCESSIVE AMOUNTS OF DATA AND NOT EVEN REALIZE IT

Recently, BKJ Digital assisted one of our clients in the Cybersecurity industry with managing this exact issue.

Due to the fact that the client worked in Cybersecurity, their reputational risk of a potential breach in their customers' data was very high. There was no cataloging process put into place to monitor PII when their systems were designed, so they were retaining excessive amounts of data that wasn't being used for any purpose.

The client had been running a successful customer-facing application for several years, and a substantial amount of customer PII had accumulated in their system over the application's normal course of use.

The scope of their PII had grown to a point where it included millions of customer data records. An amount that was so high, it would certainly make headlines if a breach were to occur, even though it wasn't considered 'critical' data, like medical or financial information.

And yet, there was no process in place to regularly evaluate and remove PII that wasn't adding value to their business. This resulted in their PII to continue growing, far above and beyond the point where the majority of the data was of any use.

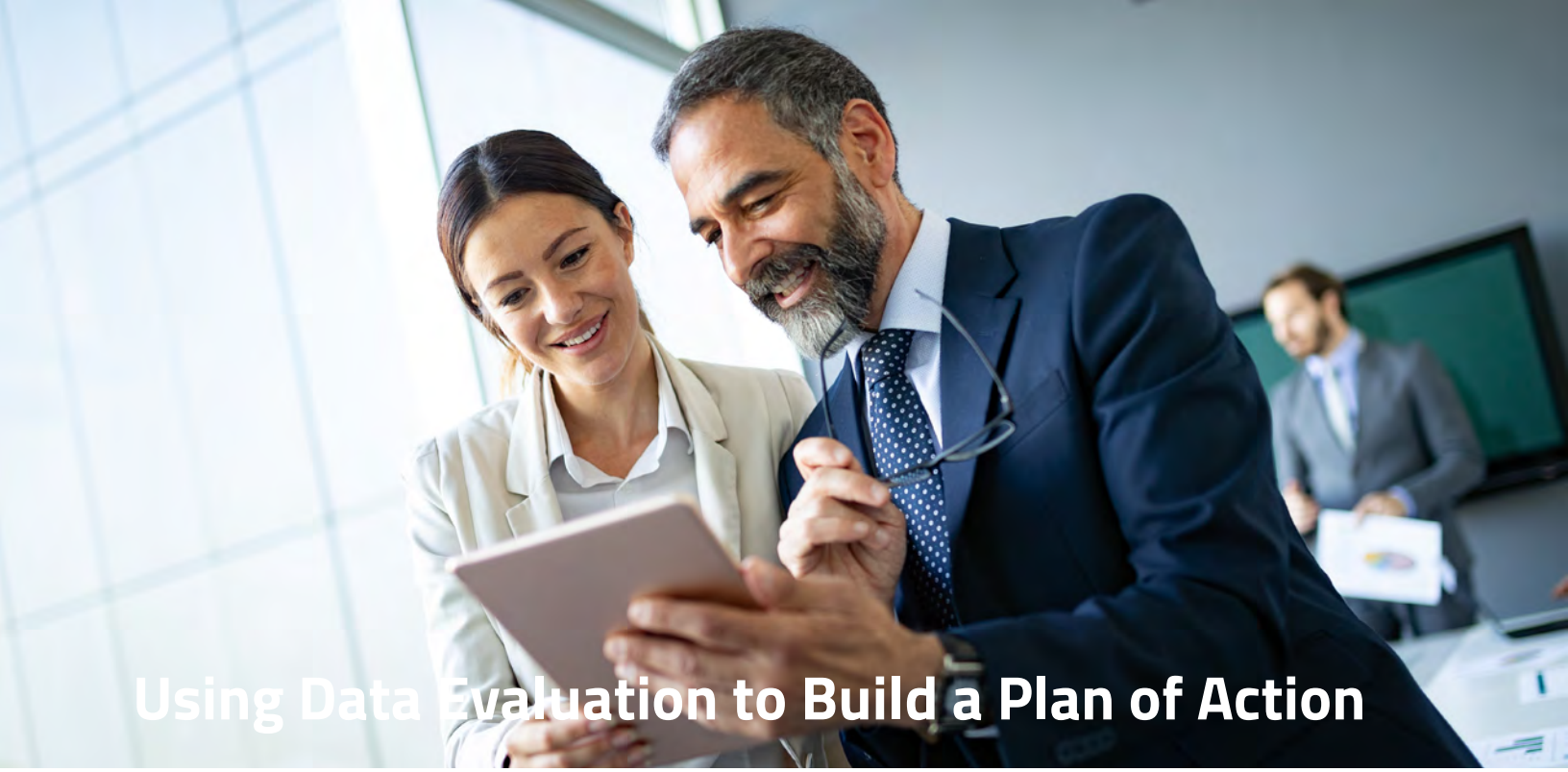
EFFECTIVE PII REDUCTION AND HYGIENE POLICIES CAN LEAD TO MORE EFFICIENT DATA USAGE

The client had no idea that this volume of PII was substantially increasing their risk of damage brought on by potential leaks in data.

They were focused on the operations of their business, and it wasn't until we brought the issue to their attention that they realized just how serious the ramifications would be, if a leak were to occur.

Once they were made aware of the issue, the mountain of data they were sitting on became apparent. With the potential risks clearly defined, the client decided that they wanted to do something to reduce their PII retention, but they weren't sure where to start.

This is where BKJ Digital was able to assist with a simple, proactive solution.



Using Data Evaluation to Build a Plan of Action

LOW-VALUE PII CARRIES THE SAME REPUTATIONAL RISKS AS HIGH-VALUE PII

After the sheer volume of their collected PII was brought to their attention, the client immediately agreed that they wanted to reduce the amount of PII in their systems.

While the types of PII they were collecting were fairly low-value (non-medical and non-financial), the client understood that when breaches occur, headlines discussing the topic rarely include any kind of value-based nuances.

"Company X suffered a breach of 3 million customers' PII today, but it was only email address and names, so it wasn't a big deal", isn't a headline you'll ever see in the news.

The client understood the seriousness of the reputational risks caused by the mass amount of data in their system, so they contracted BKJ Digital to help create actionable, long-term solutions to their PII retention issue.

WE REDUCED THE CLIENT'S PII SIZE FROM 3+ MILLION RECORDS TO LESS THAN 200K

OFFERING MUCH-NEEDED SUPPORT FOR PRIVACY TEAMS

The first step towards reaching a solution involved measuring the true scope of the PII in the client's system, so that we could provide their privacy team with context and specifics relating to the size and types of data being retained.

After the scope had been clearly identified, we worked alongside the client to create a new retention policy based on the business value of PII they wanted to keep. This way, we could ensure that low-value data that's old/stale would be removed from the system and would continue to be downsized moving forward.

With a new policy in place, we implemented automation to keep retained PII at a minimum in the future, while also reducing the backlog of older PII in the system.

When we'd finished implementing this new strategy, the client's retained PII size was reduced dramatically – from over 3,000,000 customer records to less than 200,000 records (each customer record included several pieces of personal customer data).

Are You Ready to Take Back Control of Your PII?

TAKE A PROACTIVE APPROACH TO PII MANAGEMENT AND AVOID THE AFTERMATH

Data leaks are an unfortunate part of the digital age, and sadly, the bigger your brand becomes, the bigger a target your enterprise becomes for hackers. It's vital to remember that you don't have to wait until you're dealing with fallout from a data breach, before you take steps to protect your customers and your business.

We believe in providing a proactive approach to solutions. This example isn't the only situation in which we've been able to excite a privacy team.We approached them ahead of any data breaches with a plan to not only reduce but better manage their incoming/retained PII, while also optimizing the impact of their marketing efforts.

Most companies are used to waiting until there's a major problem to solve (like a data breach), before they make changes to policies and properly address these issues. Just like many marketing teams are unaware or ignore 'innocent' data collected as part of their marketing strategies, as well as the hidden dangers they present.

This isn't conducive to finding the best solutions. Once a breach has occurred, the damage has already been done. Finding a solution after the fact may prevent it from happening again, but the financial and reputational damage incurred because of a breach can't be undone.

That's why we believe it's always best to identify and resolve these issues ahead of problems, so that if/when breaches do occur, the damage is already minimized. Instead of facing consequences after the act, you can be a hero by partnering with privacy teams in advance.

DON'T LET YOURSELF BECOME A TARGET

When data breaches occur and people get litigious around GDPR breaches, it's not often you'll see lawsuits levied against small companies with minimal PII.

The major targets are the enterprise companies that are dealing with hundreds of thousands or millions of pieces of customer data. Stacking tons of unnecessary PII in your system indefinitely could be considered equivalent to putting a target on the back of your business.

Every piece of PII you retain that offers no business value only succeeds in adding the potential risks and liabilities your company could face in the event of a breach.
Too much useless data in your systems makes it more challenging to identify and take advantage of data that is valuable.

So, you have to ask yourself: can I demonstrate leadership internally by proactively partnering with a privacy team to deal with data concerns? Have I considered the potential hidden risks of my marketing efforts?

If so, it's time to think about changing your policies and procedures to improve your protections. Are you ready to take back control of your customer PII? We can help.

ABOUT

BKJ DIGITAL

BKJ exists to empower marketers on their journey of Digital Transformation. We specialize in delivering smarter internal systems, and stronger customer experiences, to support the unique needs of enterprise organizations.

OUR CORE SERVICE OFFERINGS INCLUDE

PLATFORM INTEGRATION & MODERNIZATION

We bring existing tools up to current standards, get your platforms talking to each other, integrate 3rd party platforms, develop custom software, and implement new enterprise technology.

CONTENT STRATEGY & PUBLISHING

We build frictionless partner portals, DAMs, publishing systems and customer communities. From search and content aggregation solutions to maximizing PII data security, we'll optimize the value and discoverability of your content.

USER EXPERIENCE DESIGN & DIGITAL BUILDS

We create integrated app and website experiences. Through strategic consulting, solution planning, UX, visual design, and a complete suite of development/testing/hosting, we build custom experiences centered around your user.

We've worked closely with enterprise marketers in streamlining, building, and delivering award-winning internal and customer-facing digital experiences. If you are looking to maximize your enterprise productivity, leverage the value of your content, or build user-centric digital experience, let's talk.