PUBLICATION

Data Breaches: The Not-So-Hidden Cost of Doing Business

Authors: Matthew George White, Alexander Frank Koskey, III, Justin S. Daniels
October 14, 2024

In this era of big data, smart devices, and constant connectivity, the clock's already ticking on your next data breach – it's just a matter of time. For companies of all sizes and across every industry, the stakes have never been higher. A data breach can leave a trail of financial, legal, operational, and reputational damage that feels like trying to outrun a speeding freight train – spoiler alert: it's not going to end well. Many studies, including IBM's annual *Cost of a Data Breach Report,* make one thing clear: cyber incidents are becoming more frequent, costlier, and more difficult to manage.

So why should you care? Well, beyond the hefty price tag (which has gone up 10 percent this year alone), it's the hidden costs like customer loss, reputational impact, operational downtime, and post-breach headaches that can sting the most. And for businesses handling sensitive customer data, there's no "get out of jail free" card. But don't lose sleep – we've got your back. This summary breaks down the numbers and key findings from IBM's latest report and provides our recommended takeaways to help you start thinking ahead – because in cybersecurity, as George Washington (and later Bill Belichick) have articulated: the best offense is a good defense.

Key Findings

1. The Cost is Rising, and You're Likely Paying for It

The average cost of a data breach globally jumped **10 percent** to a staggering **$4.88 million** in 2024, marking the steepest increase since the pandemic. But the real eye-opener? More than **63 percent of companies** are passing these costs along directly to consumers through price increases on their products and services. So, the next time your coffee costs a little more, it might just be because of someone's data breach.

Baker Donelson Takeaway: Data breaches are not just a cybersecurity issue – they're a critical business issue. Costs are rising, and businesses often push that burden onto their customers, potentially impacting brand loyalty.

2. AI to the Rescue: Cutting Costs With Automation

Organizations that implemented **AI and automation** in their security operations saved an average of **$2.2 million** per breach. These tools help detect and respond to threats faster, reducing the time attackers have to wreak havoc within corporate networks.

Baker Donelson Takeaway: Investing in AI isn't just a tech upgrade; it's a cost-saving opportunity. AI tools can detect and neutralize breaches faster, mitigating both financial and reputational damage. However, careful consideration must be given to vetting AI tools and your organization's AI data governance program to ensure you are not only using the correct tools, but also using those tools in the correct (safe and compliant) manner.

3. Breach Lifecycles: the Longer It Drags On, the Worse It Gets

When a breach involves **stolen credentials** (think weak passwords [e.g., "ABC123" or "Password"] or phishing attacks), it takes an average of **292 days** to identify and contain it. For perspective, that's over 100 days longer than the average Major League Baseball season. Meanwhile, malicious insider attacks – where an employee goes rogue – carry the highest price tag, costing companies **$4.99 million** on average.

Baker Donelson Takeaway: Time is money and the longer a breach goes undetected, the more expensive it becomes. Investing in early detection tools is essential to limit the financial impact.

4. Customer Data at Risk: the Most Common Target

Nearly half of all breaches (46 percent) involve **customer personal data**. PII (Personally Identifiable Information) breaches are particularly expensive, costing **$173 per record** on average, up from $156 in 2023.

Baker Donelson Takeaway: Protecting customer data is crucial—those breaches are costly, and the longer the data is exposed, the higher the risk to your bottom line. This is especially true given that the data breach class action litigation floodgates have opened. Moreover, when you include the operational impacts caused by these breaches, such as hospitals being forced to turn away patients, financial institutions being unable to service customer accounts, or payment processors being unable to process payments, the costs, consequences, and repercussions from these incidents have never been more significant.

5. Recovery is Slow – Really Slow

Full recovery from a breach is no quick fix. Less than **12 percent** of organizations reported full recovery in under 100 days, and most organizations still aren't fully recovered by then. Business disruption, reputational damage, and long-term compliance issues prolong the pain.

Baker Donelson Takeaway: Be prepared for the long haul. Recovery from a data breach doesn't end when the hackers are gone – it can take months (or longer) to fully get back on track. Properly planning for these issues can make a dramatic difference in recovery times.

6. Ransomware and Extortion: To Pay or Not to Pay?

Organizations that involved law enforcement during ransomware attacks saw **$1 million** in savings compared to those who tried to handle things internally. Even better, **63 percent** of organizations that called in law enforcement managed to avoid paying a ransom altogether.

Baker Donelson Takeaway: Talk to your legal counsel about involving law enforcement early in your response to an incident. It can significantly reduce both the financial and legal fallout of a ransomware attack and might save you from having to make that painful ransom payment.

7. Cloud and Shadow Data: The Hidden Costs

Breaches involving **public clouds** were the most expensive, averaging **$5.17 million**. And **35 percent of breaches** included **shadow data**, or data that is stored outside of authorized channels, often without proper oversight. Shadow data breaches cost 16 percent more than those without.

Baker Donelson Takeaway: As companies move to cloud environments, they must pay special attention to the growing issue of shadow data, which complicates detection and drives up costs.

Our Advice: "Expect the Best, Prepare for the Worst"

The data breach landscape is evolving rapidly, and the findings in this report are a wake-up call for organizations of all sizes. Data breaches aren't just an IT problem – they're an existential threat to businesses, especially when costs are skyrocketing, and consumers are increasingly paying the price. The key takeaway? You can't afford to skip the critical investments in AI, automation, and robust cybersecurity. But just as important, you need the right legal strategy to guide those efforts – and that's where we come in. These efforts not only protect your bottom line but also safeguard your reputation in a world where trust is more fragile than ever.

Think of cybersecurity as a company-wide initiative, not just an IT project. The longer you wait to act, the bigger the risks – and the bills. By staying ahead of the curve with proactive tools and strategies, you can keep your organization safer and more resilient in the face of inevitable breaches. After all, when it comes to cybersecurity, fortune favors the prepared.

Don't Wait Until It's Too Late – Reach Out Today!

Whether you have questions about your current cybersecurity setup, want a second pair of eyes on your privacy programs, or just want to make sure you're prepared for the latest cyber threats, we're here to help. Don't let these issues keep you up at night – give us a call and let's make sure your business is ready to face whatever comes next. You can reach out to the authors – Matt White, Alex Koskey, Justin Daniels, or any member of our Baker Donelson's Data Protection, Privacy, and Cybersecurity Team, and we'll guide you through your next steps. Ultimately, when it comes to cybersecurity, a little foresight can save a lot of regret – and the right legal team makes all the difference.

Remember after all: "The future is not set. There is no fate but what we make for ourselves." – "Terminator 2: Judgement Day"