What IBM's 2024 Report Tells Us About Data Breaches and Lawyers

Written by Kate Rattray

IBM Security recently released its 2024 Cost of a Data Breach Report. This report studied 604 organizations that experienced data breaches between March 2023 and February 2024 to help IT, risk management, and security leaders understand the impact.

Why should lawyers pay attention to this report on data breaches?

According to the American Bar Association's *2023 Legal Technology Survey Report*, nearly 30% of law firms reported having experienced a security breach.

In our increasingly interconnected society, and in a profession that demands data security, lawyers simply can't afford a data breach. Yet, over one-quarter of firms report that they've experienced one.

Below, we'll provide some highlights from IBM's 2024 Cost of a Data Breach Report and delve into how lawyers can avoid a data breach.

Watch our webinar on Legal Cyber Security here for even more actionable tips on how to protect your firm.

Highlights from IBM's 2024 Cost of a Data Breach Report

The 2024 Cost of a Data Breach Report studied 604 organizations impacted by data breaches between March 2023 and February 2024.

The average cost of a data breach has increased

According to IBM, the global average cost of a data breach has risen to $4.88 million. This amount is the highest ever reported and represents a 10% increase from the previous year.

For professional services organizations (including legal, accounting, and consulting firms), the cost of a data breach is even higher, with an average cost of $5.08 million.

Organizations aren't often discovering data breaches themselves

Unfortunately, organizations that experience a data breach aren't often the ones to discover the breach.

According to IBM, 42% of data breaches were discovered by the organization itself (an improvement from 2023, when only one in three data breaches were identified by the organization itself). Thirty-four percent of data breaches were discovered by a neutral third party (such as law enforcement), while 24% were disclosed to the organization by an attacker.

Artificial intelligence can help

Using security artificial intelligence (AI) and automation can help organizations increase detection and response times to data breaches—and consequently decrease breach cycles—and help organizations save on costs.

Organizations that used security AI and automation saw, on average, significantly lower breach costs. Those not using AI and automation had average data breach costs of $5.72 million, while those making extensive use of AI and automation had average data breach costs of $3.84 million—a difference of $1.88 million.

Organizations leveraging security AI and automation also identified and contained data breaches nearly 100 days faster than those that don't.

Learn more about AI and security in our piece, Exploring the Intersection of AI, Cybersecurity, and Privacy.

What does a data breach look like for lawyers?

A data breach is, essentially, any security breach that results in unauthorized access to confidential information.

Within a law firm, a data breach can arise in several ways, including:

- Lost or stolen hardware (e.g., where an unencrypted work laptop is stolen from an employee's car)
- Cyberattacks (e.g., malicious attacks by cybercriminals)
- Employee error (e.g., where an employee unintentionally discloses confidential information)

While data breaches can be devastating in any industry, lawyers' unique ethical obligations make data security especially critical for their organizations.

Why lawyers must take data breaches (and data security) seriously

Lawyers have an ethical duty to protect their clients' information and to disclose data breaches. As outlined in our 2024 Law Firm Data Security Guide, lawyers should "make reasonable efforts to prevent the inadvertent or unauthorized disclosure of, or unauthorized access to, information relating to the representation of a client" under ABA Model Rule 1.6: Confidentiality of Information.

Additional breach notification requirements may apply depending on your location or practice area, including HIPAA (for lawyers handling personal health information), GDPR (for lawyers handling personal information belonging to EU residents), or your state bar's data privacy compliance requirements.

But what about the consequences of a data breach?

Beyond the high financial cost of a data breach outlined in the 2023 report, data breaches can have other significant impacts on law firms. This can include a loss of trust in your firm and malpractice lawsuits.

Learn how to protect your law firm in our on-demand webinar, Legal Cyber Security: How to Protect Your Firm Against Rising Threats.

Protecting your law firm from a data breach

Avoiding data breaches doesn't happen overnight. Law firms must invest heavily in security, including vetting their software vendors carefully.

Clio is proud to provide industry-leading security, including dedicated security experts who are available 24x7x365 to respond to data breaches and other security events. Clio adheres to industry best practices (such as HTTPS and TLS) and complies with GDPR, HIPAA, and PCI legislation. Furthermore, Clio's data hosting facilities are audited annually for SOC2 and ISO27001 security certifications. Book a demo with Clio to learn more.

At the end of the day, no law firm can guarantee that a data breach won't happen.

However, prevention is the best method of minimizing your risk. By working with software providers like Clio that are not only committed to data security but understand the unique compliance requirements law firms must follow, you can protect your firm and clients from the unexpected.

And, if you're looking for further data security insights, be sure to check out our guide to Cybersecurity for Lawyers!

About Clio

Clio is the global leader in legal AI, powering legal work across the profession, from law firms of every size to corporate legal teams, government agencies, and courts. Its Intelligent Legal Work Platform unites the business and practice of law, connecting the people, information, and processes behind legal work. Clio's AI brings the context together with legal sources drawn from Clio Library, a growing collection of more than one billion legal documents. Over 400,000 legal professionals in more than 130 countries rely on Clio to run their legal world. Learn more at www.clio.com.