Law Firm Data Breach: What To Do When The Worst Happens

Data Breach

“I am convinced that there are only two types of companies: those that have been hacked and those that will be. And even they are converging into one category: companies that have been hacked and will be hacked again.”

Then-FBI director Robert Mueller shared these sobering words at the 2012 RSA Cybersecurity conference. When it comes to a data breach, it’s not a matter of *if* but *when* and *how bad*. These words aren’t exactly encouraging. It’s as if he believes a data breach is inevitable.

He’s right.

But most firms aren’t prepared for this reality. Many legal professionals prefer to roll the dice. They still assume it can’t or won’t happen to them.

Most firms aren’t prepared for a data breach

The LogicForce Cybersecurity Scorecard states **53%** of firms have *no disaster response or recovery plan* in place. **60%** of firms don't have a security and compliance officer and what's worse, *they have no plans to hire one*. **77%** of these firms have *no cybersecurity insurance*.

These firms are exposed.

Large firms may be able to take the financial hit from a data breach or adverse cybersecurity event, but what about smaller firms? Can they afford to take the hit? Data from the ABA Tech Report suggests that the answer is no.

Are they prepared for an attack? An ILTA survey showed:

- **87 percent** of law firms do not encrypt laptops, netbooks and mobile devices
- **61 percent** don't have intrusion *detection* tools in place
- **64 percent** don't have intrusion *protection* tools
- **40 percent** of firms *weren't even aware* an attack had occurred
- **22 percent** have a documented cybersecurity training program
- Only **23 percent** have cybersecurity insurance policies in place

The majority of small-to-medium law firms aren't prepared to recover from the inevitable attack headed their way.

The law firm data breach: How to recover

Let's imagine that the inevitable has happened. A disgruntled insider or predatory outsider has broken into your company. What are the steps you should take to recover from an adverse cybersecurity event?

Step 1: Secure your network/data

You'll want to take steps to lock down your data, traffic and network. You'll also want to verify that the right employees have access to the right data, at the right time.

1. **Notify your IT or data, forensics team.** Request that they conduct a thorough investigation. If your firm has multiple departments, you'll want to make sure you have the appropriate teams on deck and ready to help.
2. **Consult with your resident experts.** If you don't have an in-house expert you can lean on you'll want to reach out to a trustworthy third party that can provide your firm with the legal counsel needed.

3. **Lockdown physical access.** Any areas related to your breach should be locked down and monitored carefully. You'll want to change any access codes, locks, or credentials needed. If you have multiple employees, you'll want to reach out to local law enforcement to determine when it's safe to resume day-to-day operations.
4. **Prevent further data loss.** If you've already lost important data, you'll want to take the appropriate steps needed to lock things down further. If there's any evidence present in the breach, you'll want to take special precautions, so you don't destroy any important pieces of evidence.

These details are important steps you should take immediately after a breach or cybersecurity event. You'll want to focus your attention on limiting the amount of data flowing out of your firm.

Step 2: Fix, patch or update your vulnerabilities

1. **Identify the source/cause of the breach.** You'll want to identify when, how and why these attackers were able to get into your organization. The IT or data forensics team you've identified in step one should be able to help you identify the cause of the breach.
2. **Vet third-party providers.** Do third party providers have access to your data via an API or another piece of software? You'll want to verify that:
    - Your providers should have continued access to your data.
    - That your provider's system is secure and any vulnerabilities have been patched.
3. **Cooperate with IT and your forensics team fully.** You'll want to identify:
    - Which security measures were enabled at the time of the breach
    - Analyze whether you (or a third party) were able to contain any or all of the breach successfully (e.g., via network segmentation.
    - Assess user rights management and current group policies to verify the right people have access to the right pieces of data, at the right time.
4. **Create a crisis management plan.** You may need to provide the right people – clients, employees, suppliers, providers shareholders, partners and the public with the appropriate level of communication. Your communication and crisis management plan should
    - Own the mistake or mishap.
    - Not withhold key pieces of data from your audience.
    - Not withhold or share information that makes it harder for clients to protect themselves.

Create a list of the questions, objections, fears, and concerns each audience will have. Provide them with details on what you've done or are doing to address the problem.

This is an important first step. If you take the time to approach this area carefully, you'll be able to recover your reputation and limit potential losses ahead of time.

Step 3: Notify your relevant parties

You'll need to notify the various groups of people mentioned above about the breach. You'll want to ensure that you're fully compliant with any and all laws, whether they're at the local, county, city, state or federal levels. As you know, most states will have specific requirements for releasing information.

If the breach involves health care data, you'll need to determine whether you're required to comply with the *FTC's Health Breach Notification Rule* or the *HIPAA Health Breach Notification Rule*. These rules will outline who needs to be notified (e.g., the media) and when.

You'll also want to notify affected (clients) businesses. If the breach affects a significant or large group of people, you'll need to notify credit bureaus.

A data breach is inevitable; catastrophic data loss isn't

The law firm data breach is something your organization can recover from. Create a recovery plan, follow the above steps and you'll have what you need to restore your business and your reputation to full working order.