Beat the Clock Following a Data Breach

There are legal requirements your firm must meet after a breach — do you know what to do?

MARK BREWER
Freelance Writer

Cyberattacks are commonplace — every law firm has experienced an attack in one form or another. While most attacks don't result in the exposure of information, those that do present a risk to law firms.

All attorneys and firms are privy to sensitive client data, so they are ripe targets for hackers. "Law firms are a treasure trove of personally identifiable information," says Kris Wasserman, Regional Vice President at Special Counsel, a provider of legal technology and e-discovery solutions. And hackers mine that personal data to steal identities.

If you feel a sense of security being a smaller firm, you shouldn't. While a recent ABA study revealed that one in four law firms with 100 attorneys or more reported cyberbreaches that resulted in the exposure of data, 52% of firms with 10 to 50 attorneys experienced similar breaches — more than twice the rate of larger firms. It's an eye-opener for small firms and solo practices.

In the event of a data breach where personally identifiable information is exposed, all law firms are required by law to notify affected individuals in a timely manner.

A PATCHWORK OF LEGAL REQUIREMENTS

Nearly every business or law firm must conform to breach notification laws. However, the

If you feel a sense of security being a smaller firm, you shouldn't … 52% of firms with 10 to 50 attorneys experienced similar breaches — more than twice the rate of larger firms.

legal requirements for notification are complicated. Each state has its own rules on when and how to notify.

"The state where the affected people live will determine what triggers the duty to notify, the form of notice and how much time you have," says Wasserman. "Each state defines personally identifiable information differently. Each state defines what constitutes a breach a little bit differently. Each state has their own exemptions and rules about the form of the notification and the types of businesses that must comply."

In addition to state laws, legislation like the Health Insurance Portability and Accountability Act (HIPAA — the federal law restricting the release of health information) and the Gramm-Leach-Bliley Act (the federal law requiring financial institutions to explain how they share and protect their customers' private information) may apply if your firm handles the type of data covered by these laws. The European Union's General Data Protection Regulation (GDPR) applies if personally identifiable information of EU citizens is exposed. And client service agreements may also have provisions — something that is increasingly becoming more popular, according to James Harrison, Chief Executive Officer of INVISUS, a cybersecurity company with law firm experience.

THE CLOCK IS TICKING

The common theme among all legislation is that the notification clock starts when a breach is discovered. At that point, you have somewhere between 30 and 60 days to have notifications in the mail to each affected person. Failure to notify on time will get your firm into hot water, including the possibility of significant financial liability or reputational damage.

Uber and Equifax waited months to report their highly publicized breaches and, as a result, both company's management teams were dismantled and both suffered stock devaluations. Due to the gravity of some notification laws, law firms that don't act quickly on the requirements can fail within months following a breach, according to Harrison.

BE DEFENSIBLE: HAVE A PLAN

The tricky part is, how do you meet all the individual state obligations in 30 to 60 days when you have 50 sets of rules?

"Be prepared to be defensible with a response plan that's documented, thorough and practiced," says Harrison. With such a plan in place, "responding to a breach becomes much simpler and offers much more protection for the reputation and the financial risk to the firm," he says.

Being prepared involves understanding what kind of data you store, which states or countries you do business in, and which states or countries your clients do business in. You'll need to know the rules for each state or country.

Being prepared involves understanding what kind of data you store, which states or countries you do business in, and which states or countries your clients do business in.

Firms can do this work on their own or hire a specialist to sort this out. But the most convenient path is to carry cyber insurance. Insurance carriers are experts in the notification process and have quick access to response experts, including forensic teams that determine if a breach requires notification and legal experts to sort out when and how to notify.

HOW TO RESPOND TO A DATA BREACH

Regardless of the path you choose, there are several steps in the process.

1. **Preserve the evidence:** Don't overwrite or delete anything. Secure it for investigation.
2. **Initial discovery:** Do a quick investigation into suspicious activity and validate that a breach has occurred. In general, potential exposure or theft of information qualifies as a breach.
3. **Containment:** Take steps to contain the problem and prevent more loss. If necessary, isolate affected computers from the network.

If Uber and Equifax are valid lessons, then the health of your law firm post-breach will depend less on the fact that you were breached and more on your ability to meet the legal requirements to respond.

4. **Contact your cyber insurance carrier or an expert:** If you have cyber insurance, your insurance company has response teams in place and ready to go, including experts in computer forensics and state law. They will guide you through the process.

5. **Deeper discovery:** Dig deeper to determine the full scope of the breach and whether personally identifiable information was exposed. If so, the next step for your firm, expert or insurance carrier is to sort out whether the breach requires notification based on state laws or federal regulations.

6. **Take corrective action:** Once a breach is confirmed and the scope of the breach is determined, you can clean and restore affected computers and devices, apply security updates and patches, or implement other safeguards.

7. **Notify individuals:** If the breach meets a legal standard for notification, you must mail notifications by the deadline, and it must follow the form required by the applicable laws. Notifications are generally specific as to the type of data exposed — such as Social Security number, date of birth or credit card numbers — and the type of remediation required by law, such as credit monitoring for a specific period of time. Your firm, expert or insurance carrier writes the notification based on applicable laws and produces and mails the notifications.

8. **Notify government authorities:** Typically, if data for 500 or more individuals is exposed, you're required to contact the state attorney general or other authority. Be aware that some states require this for a breach that exposes any number of individuals.

9. **Control the message:** For large breaches, some states and regulations require public notification through the press. But it's a good practice for firms to control the message in order to preserve the firm's reputation.

FOLLOW BEST PRACTICES

Attacks are constant and mistakes happen, even in the most secure environments. The best defense against the legal fallout following a breach of personal data is to follow best practices in securing your environment, which includes having a plan in place to respond to a possible future attack.

If Uber and Equifax are valid lessons, then the health of your law firm post-breach will depend less on the fact that you were breached and more on your ability to meet the legal requirements to respond. ■

ABOUT THE AUTHOR

Mark Brewer is a freelance writer who helps decision-makers understand technology, trends and ideas to make them more effective in their work.

mark@markbrewerwriter.com
markbrewerwriter.com
815-565-7272