centerbase.com

Centerbase CloudBased Law Firm Management & Growth Platform

Before, During, and After: Ensure Your Law Firm is Prepared to Address a Data Breach

developers · Tuesday, August 31st, 2021

When law firms are impacted by a cyber attack, they must take immediate steps to address the data breach and minimize its impact. While these tasks generally occur in the days following an event, the most effective response requires the existence of an incident response plan *before* an attack occurs. By contemplating the potential impact of these disruptive events ahead of time and crafting a plan, law firms can be better prepared to respond.

Read on for a checklist of steps that law firm attorneys and administrators alike can take to appropriately respond to a data breach:

Incident Response Plan

According to the ABA's most recent Legal Technology Survey Report, only about a third of respondents have an incident response plan in place. Yet, the ABA notes that incident response plans are critical to law firm operations, providing firms with a roadmap of steps to take when a data breach occurs. These plans require a significant amount of preparation, but the effort is worth its benefit should a breach occur.

There are numerous models for law firms to follow when crafting their own incident responses, but every plan should include these general provisions:

- A reporting mechanism for firm members to quickly report suspected incidents.
- A detailed plan for the investigation and minimization of business disruption.
- Recovery requirements for the testing and validation of all systems before continued usage.
- Detailed notification procedures.
- Training and drills for firm staff to reduce incidents involving human error.
- A mandatory hindsight review of any incident to determine cause and address weaknesses in the incident response plan.

Stop the Breach and Mitigate

Formal Opinion 483 of the ABA Standing Committee on Ethics and Professional Responsibility states that "when a breach of protected client information is either suspected or detected, Rule 1.1 requires that the lawyer act reasonably and promptly to stop the breach and mitigate damage resulting from the breach."

Stopping the breach may entail a number of different steps, including:

- Removing the hacking tools.
- Notifying the appropriate authorities.
- Securing any physical areas related to the breach by locking them and changing any relevant access codes.
- Taking all affected equipment offline without destroying evidence.
- Updating credentials and passwords for authorized users.

Once the breach has been stopped, firms need to take “all reasonable efforts” to restore operations and resume client services.

Analyze the Occurrence

Then, firms should next take steps to determine how the data breach occurred, which may require the assistance of a tech expert. Attorneys and administrators should ask probing questions, such as:

- Who had access to the data at the time of the breach?
- What type of information was compromised?
- Was encryption enabled at the time of the attack?
- Whose data was impacted?

The information and evidence gathered can be used to ensure that the current breach has been effectively stopped, while also helping to identify what steps can be taken to prevent future attacks. An analysis of the lost or accessed data also promotes honest and transparent disclosure of the breach to clients and other impacted parties.

Address Vulnerabilities

After the problem has been identified, firms must move quickly to address it. Affected systems need to be secured and vulnerabilities removed. The appropriate tasks depend on the nature of the breach. For example:

- If the firm’s website was involved in the attack, it should be taken offline immediately.
- If the breach involved a third-party service provider, firm leaders should consider whether access privileges should be modified. If the provider claims to have remedied the issue, it is still the firm’s responsibility to verify that the problem has been addressed.

Contact Impacted Parties

When identifying impacted parties, firms should analyze the type of data that was compromised. Did the data loss include the last name of a person along with at least the first initial of the first name? Did it include social security numbers or tax ID numbers? Were financial accounts, credit card data, drivers license numbers, or medical information compromised? If any of these details were stolen, then the impacted person or business should be notified.

Under most state ethics rules, attorneys generally have a duty to notify impacted clients of cyber incidents, particularly when the breach compromises confidential information or impairs the law firm’s ability to provide legal services. Though notification to former clients is not specifically addressed in many jurisdictions, law firms may still have a duty to notify them if their data was

impacted.

But the duty to inform also extends from general state laws concerning data breaches. For instance, a breach of clients' personal health records may fall under the Health Breach Notification Rule, which could require notification to the Fair-Trade Commission (FTC) as well as the media. This type of breach may also trigger notification requirements under the Health Insurance Portability and Accountability Act (HIPAA).

Firms need to comply with all federal, state, and local laws in notifying impacted individuals and businesses. States differ in the amount of time given to provide notification, but most typically set a 60-day limitation.

Details typically included within notifications include:

- What confidential information was breached.
- How the attack occurred.
- Any known information about how the stolen data has been utilized.
- Actions taken thus far to remedy the situation.
- Steps being taken to protect impacted individuals, such as complimentary credit monitoring.

It is also useful for law firm attorneys or administrators to consult with any law enforcement working on the case to ensure that the information provided does not hinder the investigation.

The FTC offers the following advice for businesses when notifying impacted parties:

- Use letters, websites, and toll-free numbers to communicate with people whose information may have been compromised.
- Offer guidance on what steps parties can take to protect themselves. For instance, individuals with stolen Social Security numbers should request credit freezes from the credit bureaus. For stolen banking data, parties should notify their respective banking institutions.
- Encourage parties to contact the FTC through www.identitytheft.gov should they learn that their data has been misused.
- Provide information about how communications will occur in the future to help parties avoid phishing scams that may occur from the breach.

Following Up

A cybersecurity data breach is not over once the initial disruption is addressed. These incidents have lasting effects and law firms can continuously support impacted parties by taking the following steps:

- Provide consistent notifications about material developments in the investigation.
- Designate a point person within the law firm for ongoing communications about the breach.
- Offer at least a year of free credit monitoring and/or identity theft protection to impacted parties.

This entry was posted on Tuesday, August 31st, 2021 at 12:00 am and is filed under Compliance & Security
You can follow any responses to this entry through the Comments (RSS) feed. Both comments and pings are currently closed.