How to handle document review and data identification after a breach

Today most organizations digitize all of their business information, which unfortunately increases the risk for data breaches. Massive data breaches are becoming more prevalent because of the increase in both digital data and sophisticated hackers. These breaches threaten an organization's data management and retention capabilities, business operations, and client relationships. Even organizations with top-notch security systems can be at risk for breaches. It is better to assume that no one is immune from these attacks. Implementing clear incident investigation and breach response plans is crucial to limit the consequences that could result from a substantial data breach.

Potential exposure risks

Massive data breaches can have long-lasting effects on an organization's reputation if they are not dealt with expeditiously, sensitively, and competently. These breaches can result in exposure of confidential client information, personal identifiers, trade secrets, and other sensitive business data. As such, after a breach occurs an organization faces serious consequences, including:

- Individual lawsuits or class actions
- Investigation into the organization's security program
- Hackers selling confidential client or business data
- Delay in business operations
- Loss of current and future clients
- Bad publicity

All of this will cause an organization to lose a significant amount of time and money, and could even force restructuring or dissolution. To avoid or limit the risk for negative exposure, organizations should have a comprehensive protocol in place regarding how to review, organize, and identify relevant and compromised data after a breach.

Contact legalsolutions@epiqglobal.com

Responding to Data Breaches and Streamlining Review

After an organization becomes the victim of a cyber attack, the first thing that needs to be done is a thorough incident investigation. This entails determining whether a breach actually occurred and then identifying the extent of the breach. After an organization confirms the incident and identifies the affected data, it will need to carry out their breach response plan. This step will vary based on the scope of the incident, but generally includes stopping the threat from spreading, notifying affected parties, and tightening network security after performing a gap analysis. Organizations should have a team in place that is trained on how to investigate and respond to breaches. Identifying a team and creating a clear protocol prior to encountering an incident will ensure that compromised data is dealt with in a competent and expeditious manner.

Document review and data identification are two key components for remedying the effects from a breach and reducing the possibility for further consequences. Reviewers will need to look at all potentially affected data to clearly identify what has been compromised. This also helps rule out information that that was not targeted or captured during the incident. Completing these tasks quickly and efficiently is imperative. This can be difficult since organizations will likely need to analyze a considerable amount of data. One way to streamline this stage is to outsource the review process to trained experts. Depending on the situation, these experts could include document review specialists, attorneys, and IT professionals.

Having third-party experts assist with document review and data identification after a breach helps to streamline the process because of the following benefits these services provide:

- **The review team will be solely focused on the task.** The reviewers will be impartial since they are not employees, allowing for clear focus on the task at hand. While some of the organization's employees will undoubtedly be involved with incident investigation and breach response, they could be biased or distracted with other responsibilities relating to breach remediation (such as public relations, client services, or ensuring that daily operations keep running), which could hinder the process.

- **The review team can handle varied data with superior accuracy.** The reviewers are experts in this type of work, which allows them to analyze a large amount of information and identify key data faster and more efficiently. Using computers and artificial intelligence software to enhance manual review will help to sort through data that appears in multiple formats, spans over different languages, or is otherwise compromised. This will reduce the risk of missing information that is important to breach notification and remediation and speed up the overall process so an organization can resume normal business.

- **The organization will be prepared for future litigation**. Ensuring that all compromised data is identified will allow an organization to determine how large the breach is and who actually needs to be notified. Utilizing expert services to employ these tasks quickly and effectively will likely reduce the risk of future litigation. However, even if litigation ensues an organization will be better prepared to defend their actions if the response was completed successfully with minimal fallout. All steps of this process should be documented in writing and all key data should be preserved to avoid legal hurdles.

- **Using expert services will decrease the time and money spent on remediation.** Expediting the document review and data identification components of incident investigation and breach response is economical, which is a major benefit since data breaches inevitably will cause other costs. This also allows the organization to focus on additional steps that need to be taken after a breach, such as notification, gap analysis, client communication, drafting new policies, and revamping security protocols.

Conclusion

After a major data breach occurs, taking every feasible step to limit fallout and maintain an organization's image is critical. Reviewing and identifying all potentially affected data are very important tasks that need to be completed immediately after a suspected attack. Since there are numerous obstacles an organization may face during this time, outsourcing these jobs to trained professionals can help streamline the process and ensure that all critical data is captured. Regardless, organizations should implement a clear plan for responding to breaches to make the recovery process smoother.