A Desk Guide to Data Protection and Breach Response - Part 4

March 6, 2014 Ronald Breaux, Tim Newman

PRACTICES Healthcare Transactions and Regulatory, Privacy and Cybersecurity, Energy, Power and Natural Resources, Social Media, Finance, Government and Public Policy, Government Contracts, Healthcare and Life Sciences, Insurance Recovery, Intellectual Property

The Clock is Ticking: Investigating and Responding to a Breach

Once your company becomes aware of a suspected data breach, time is of the essence. Losses from the breach are likely mounting, the clock is running on your organization?s legal rights and obligations, and the potential liability to claims by regulators and plaintiffs begins to expand. In this installment of our special series, *A Desk Guide to Data Protection and Breach Response*, we discuss strategies companies should implement once they suspect a data breach has occurred. The precise parameters of an investigation depend on a multitude of factors, but we recommend the following steps:

- **Assemble your team.** Your breach response plan should identify the best personnel to direct your organization?s response. A typical response team includes members of legal, human resources, information technology, and public relations departments. Given the potentially significant ramifications of a security incident, you should also consider notifying the board of directors, as well as inclusion of a director in the response efforts.
- **Contact legal counsel immediately.** Data security attorneys are experienced in investigating cyber incidents and know how to manage sensitive relationships with third parties, including forensic investigators and law enforcement. Moreover, the information prepared during an attorney-led investigation is more likely to be protected by the attorney-client privilege or attorney work product doctrine in the event of litigation. Your breach response plan should identify a firm or attorney to call and include their emergency contact information.
- **Be cautious with terminology.** In early written communications following an incident, avoid drawing premature conclusions regarding the cause of an incident and whether information has been accessed or stolen (?exfiltrated,? to data security professionals). If an investigation is ongoing, make sure that your updates and other reports reflect that reality. And avoid using the term ?breach,? which carries legal significance and assumes that information was exposed to unauthorized parties. Imprecise, inaccurate, or reckless communications during an investigation can hinder your organization?s ability to defend against charges of liability by affected third parties or regulators.
- **Consider hiring a forensic investigator.** Legal claims and defenses and liability arising from a security incident often turn on the reliability of evidence collection and analysis. Consider retaining a reputable investigator to assist in your investigation and remediation efforts. When an entity may have suffered a breach of payment card information (?PCI?), the card brands often require the entity to retain one of their approved Payment Card Information Forensic Investigators (or ?PFI?) to conduct a forensic investigation, but these vendors are closely aligned with the card brands and, even in the best case scenario, have split or dual loyalties to you and the card brands. You should seriously consider hiring your own independent forensic investigator to conduct a shadow investigation.

- **Review insurance contracts.** Some companies make the mistake of assuming that they cannot obtain coverage for breach-related liabilities unless they have cyber-insurance. However, in the absence of a cyber-specific policy, you may be covered under more general policies. Gather all of your potentially applicable policies and review their terms closely. Legal counsel can assist in identifying potential coverage and complying with applicable notice provisions. In a later installment of the Special Series, we will address obtaining coverage for a cyber incident in more depth.
- **Consider contacting law enforcement.** After the initial investigation is sufficiently complete, you should carefully consider (with assistance from experienced legal counsel) whether to contact law enforcement (if they have not already become aware of the breach). Law enforcement has access to investigative tools (for example, grand jury subpoenas and search warrants) that are not otherwise available to private sector entities, and are currently very interested in investigating cyber incidents that affect national security or have significant economic implications. However, law enforcement cannot and will not assist you in repairing damage to your computer network like independent forensic investigators can, and businesses may lose control over an investigation once law enforcement becomes involved.
- **Analyze disclosure obligations.** Release of sensitive personal information may result in notice obligations to the affected third parties, and compliance is often required within a specified (and short) period of time. Notice requirements are primarily based on a patchwork of state laws, and the residency of the affected parties determines which laws apply. If an incident potentially resulted in disclosure of personal information, as defined under the relevant state law, immediately assess your obligations and provide timely notice to appropriate recipients to avoid additional legal exposure to consumers or regulators. A recent lawsuit by the California Attorney General (see our coverage of that lawsuit **here**) highlights the importance of timely disclosure. A later installment of the Special Series will address disclosure obligations in more depth.
- **Consider the prospect of litigation.** A data breach may lead to various types of litigation or regulatory actions. For example, the organization itself may choose to sue the perpetrator to recover losses, and the breach may draw attention from criminal authorities. Additionally, affected parties and regulators may sue a victim organization for failing to protect information or provide timely notice of a breach. We will discuss litigation in more detail in several future installments of the Series.
- **Manage public relations.** Companies that suffer a cyber incident often suffer reputational harm as well. Work with your public relations personnel and legal counsel to limit the harm while at the same time ensuring your organization doesn?t open the door to additional legal liability. You should consider coordinating all communications with third parties through a single source to ensure that they are authorized, accurate, consistent, and timely. A customer hotline or website can be useful in this regard.

Data breach responses necessarily vary depending on the type of organization, the type and volume of information at risk, and various other factors. We strongly recommend that you consult with legal counsel to ensure that you are taking the necessary steps to minimize your losses.

In earlier installments of our special series, A Desk Guide to Data Protection and Breach Response, we discussed

- ***data protection and compliance issues*,**
- ***developing a data security plan*, and**
- ***obtaining cyber risk insurance*.**

In future installments, we will discuss regulatory actions, fallout litigation, and recovering losses through insurance claims. For additional information on any of these subjects, please contact a member of the Haynes Boone Privacy and Data Breach group.