Into the Breach

Tips for Effectively Partnering With Outside Counsel in the Data Breach Planning Process

BY DARIN M. SANDS

Target recently announced that the total cost of its data breach response efforts since late 2013 now exceeds $252 million (approximately $90 million of that has been offset by insurance proceeds). Such news, particularly when combined with a seemingly endless stream of new breaches, has businesses of all sizes seeking guidance on how to most effectively structure their breach response plans. With many stakeholders — CEOs, CIOs, CMOs, HR, Security, Compliance, among others — necessarily involved in the process, a frequent question that arises is what role should outside counsel play?

Unfortunately, that question is too often answered at one of two extremes: 1) either by outside counsel who present themselves as the primary (and expensive) driver of the process, often at the expense of important business, technical, public relations and marketing objectives; or 2) by non-legal stakeholders who view the primary role of legal counsel as a reactive one, only to be engaged after a breach.

Each extreme has the potential to result in costly mistakes in the event of a breach. Below are some considerations and guidelines to help strike the proper balance and utilize outside counsel effectively.

Proactively Protect Attorney-Client Privilege. In the wake of a major breach, communications will be made that can be misconstrued and taken out of context in later lawsuits or government investigations. In order to ensure that all key players can communicate freely and obtain timely legal advice, the breach response planning process must include a strategy to cloak the response effort in attorney-client privilege.

To benefit from that protection, a breach response must be: (1) formally directed by counsel; (2) confidential; and (3) made to assist counsel in providing legal advice. Any breach response plan must be designed with the above goals in mind. That means:

In order to ensure that all key players can communicate freely and obtain timely legal advice, the breach response planning process must include a strategy to cloak the response effort in attorney-client privilege.

- Outside counsel must be pre-selected and available around the clock to direct an investigation quickly after the breach;
- Counsel should directly engage any vendors (e.g., forensics specialists, public relations advisors) and negotiate those contracts in advance so that they can be entered into immediately upon a breach;
- To ensure confidentiality, a breach response plan should identify the breach response team and take steps to keep breach response communications within that circle; and
- All key members of the response team must be educated in advance regarding basic guidelines to ensure that privilege is preserved (i.e., marking communications as attorney-client privileged).

Review Key Contracts. Outside counsel can also proactively review relevant contracts to ensure that the company's rights are protected in the event of a breach. This includes contracts with cyber-insurance providers, cloud providers, payment processing companies and any other vendor that may host or play a role in the transmission of the company's data. Being hamstrung by limiting contractual rights can significantly inhibit the company's ability to respond effectively.

Interface With Law Enforcement. Cybercrime has become a top priority of the FBI and Secret Service and is becoming increasingly important to local law enforcement officials. Partnering with outside counsel who have established ties with law enforcement officials can provide the opportunity to work with law enforcement to both develop your plan and quickly partner with the necessary officials to respond to and stop a breach. Further, a company's state and federal customer notification obligations can be stayed pending a breach investigation, but the process of getting approval for such a stay requires immediate and adept negotiations with law enforcement officials.

Carefully selecting outside counsel will add an additional expense to the data breach response planning process, but when deployed in an efficient and targeted way, it can be an essential and valuable part of your data breach response efforts. ■

Darin M. Sands is a shareholder at Lane Powell, where he chairs the Firm's Privacy and Data Security Practice Group. He represents clients in a wide range of matters, including class actions, international antitrust investigations and litigation, claims involving breach of contract and fiduciary duties, claims arising out of non-competition agreements, internal investigations, privacy and data security litigation, and counseling related to electronic discovery policies and protocols and disputes. Darin can be reached at 503.778.2117 or sandsd@lanepowell.com.