Plugging the Leak: Guidelines for a Data Breach Response Plan

BY DARIN M. SANDS

Though data breaches have been on the forefront of many large company's risk management efforts for a number of years, it has become clear that the threat of a data breach is very real and touches on every business, regardless of size, and in nearly every part of the economy. A comprehensive 2013 Verizon report revealed that more than 31 percent of the data breaches in 2012 impacted businesses with less than 100 employees. Even in the face of these numbers, smaller companies may underestimate the threat they face. A relatively minor data breach could result in hundreds of thousands or even millions of dollars in potential costs.

Beyond bulking up data security protocols, there are relatively easy steps that every company can take to prepare for the worst. Foremost is the preparation of a clear data breach response plan. A 2013 study prepared for Symantec found that the average cost of a data breach in the U.S. was more than $5.4 million (approximately $194 for each record breached). That same study identified a clear data breach response plan as the number one way organizations could reduce the cost of a data breach, lowering the cost by as much as 21 percent.

These guidelines will assist in creating an effective data breach response plan for your organization:

Ensure that all relevant players are involved in developing the plan. This means not just your Information Technology ("IT") department but also at least one high-level executive, inside and outside counsel, and technical data breach response specialists. Ultimately, any response will require technical expertise and clear guidance from your business and legal leadership.

Inventory the type of personal information your organization collects, who the information is collected from (employees, customers, potential customers, children, etc.), where that data is stored and who stores it. This information is critical to determining who needs to be notified in the event of a breach. The statutory timelines for notifying those impacted by the breach are often very short and vary by state and country.

Make sure that leadership and reporting structures for implementing the response plan are clear. A failure to do so can lead to a delayed response, which can be fatal when every hour of delay can have substantial costs.

Make sure that your IT department is qualified to respond to a data breach. A failure to properly identify the scope of the breach early or to respond to that breach effectively can have devastating effects for the company's relationship with customers and its ability to defend its response in legal proceedings. If your IT department is not qualified to respond to a data breach, make sure you work with a consultant who is when developing your plan.

Have 24-hour contact information for all essential members of your response team. This includes:

1. At least two outside attorneys, in case one is conflicted or unavailable;
2. Pre-vetted breach response forensics experts that can respond to and contain the breach if your IT staff cannot;
3. Cybercrime representatives from local law enforcement, the FBI and the Secret Service, since each has jurisdiction over malicious breaches in some situations; and
4. Your data breach insurer if you have one.

Waiting until the work day begins to reach any of the above could make the difference between an effective and a failed response.

In today's world, the relevant question is not *if* your organization will be the victim of a data breach, but rather *when* it will be attacked. Even though an effective data breach plan requires an initial investment of time and money, the potential return on that investment in the event of a data breach is enormous.

Darin M. Sands is a shareholder at Lane Powell, where he co-chairs the Firm's Privacy and Data Security Practice Group, and Electronic Discovery, Technology and Strategy Practice Group. He is a litigator who focuses his practice on complex commercial disputes. Darin can be reached at 503.778.2114 or sandsd@lanepowell.com.