Data breach response: How to counsel your client

by Sandy Garfinkel

You are at your desk in your law office on a Friday afternoon when the phone rings. It is the chief information officer at ZYX Co., your long-time client. "We think we've had a data breach," he says. "We thought we were protected against this type of thing. What should we do?"

With reported data breach incidents increasing at a rapid pace (a 46 percent increase from 2013 to 2014), receiving such a call from a client is becoming increasingly likely. Answering the client's question is no simple task. A data breach is a many-headed monster. This article is intended to provide some practical advice and to highlight key issues of which you should be aware as a practitioner, but it is not intended to be an exhaustive tutorial on data breach response.

If you're fortunate, ZYX Co. already has a data breach response plan in place, and perhaps it is a plan that you or another lawyer drafted or reviewed. A good data breach response plan should provide a road map for what steps to take in the appropriate order of priority and should include lists of key people, both internal to the company and beyond, who should be involved in the response efforts.

The reality is that most companies will not have a data breach response plan in place. You will be starting from scratch, responsible for guiding your client through a maze of differing, and sometimes conflicting, state and federal laws. How should you proceed?

Identify the Particulars of the Breach and Ensure Containment

Many clients will say "We had a breach" without considering the possibility that the breach might still be occurring. Big breaches like Target and Anthem continued for long periods of time prior to detection.

The most pressing priority for your client must be to identify the breach and put a stop to it, if it hasn't already been contained. If the breach involves a compromise of computer-stored information, this step is likely to require a prompt intervention by a qualified forensic investigation firm. If the breach involves the theft of personal information in paper form, then an internal investigation may be called for, as well as a review of security procedures and policies concerning the storage of and access to such information. As circumstances warrant, the appropriate law enforcement agency should be alerted quickly and the agency may determine that a criminal investigation should be undertaken.

Determine the Who, What, Where, When and Why

Currently, with some exceptions, data breach response is controlled by individual state laws. Forty-seven states have data breach response laws on the books. All of them purport to apply when at least one of that state's individual citizens is affected by a breach, regardless of where the breach occurred or where the breached company is located. Therefore, depending upon where your customers or employees are located, a breach may trigger response obligations under a number of different state laws. Not all of these laws are consistent with each other in terms of notification content, the types of information protected, timing, and requiring notice to state regulatory bodies, among other things.

Once your client has identified and contained the breach, the next step is to understand what information was affected. If it was personal information, find out what types, the number of individuals affected and where they reside. In a breach of electronically stored information, the company's information technology department should work with a qualified forensic investigation firm to determine what devices, databases or other parts of the system were intruded upon by the breach, which will hopefully help to answer the question of what information may have been compromised.

Determine Response Duties and Execute Them

Your client reports that the breach targeted employee information and, specifically, that 400 employees' Social Security numbers were compromised, with those affected residing in 12 different states.

As ZYX Co.'s lawyer, you must review and assist your client in complying with the data breach response laws of each of those 12 states. Under all 12 of those statutes, the compromise of Social Security numbers will constitute a breach, triggering notification and response duties. However, you may find that four of the states' statutes require notification of a regulatory body, and of those four, two require that such regulator notice be sent before any affected citizens are notified. Most likely, all 12 will require that notifications be issued "as soon as reasonably practicable, without unreasonable delay." However, a few statutes require notification within a set period of time, most frequently 30 days. Of the 12 state laws at issue in this hypothetical incident, two or three of the statutes might have specific notification content requirements.

Depending upon the number of affected people, notification can be done in-house by you or your client or outsourced to a data breach response vendor. As the company's lawyer, you must "quarterback" the response efforts by reviewing the notifications for legal sufficiency, dictating the timing and method of notification, and coordinating the moving parts so that everything is handled in compliance with applicable laws and regulations. You may also recommend to your client that it provide to affected individuals, at your client's expense, an opportunity to enroll in credit monitoring and/or identity theft restoration services. Those services can be purchased from industry vendors, and regulators have expressed strong views that such services should be offered by breached entities at no cost to consumers.

Preparing for Impact

While you are assisting ZYX Co. with its statutory response obligations, you should also be preparing the company for potential fallout from the incident. As notifications go out, questions are likely to start pouring in from affected individuals who may call to complain or to learn more information about the breach; regulators may question the timing or sufficiency of the notifications sent to individuals; and the media may become aware of the incident and may want to publish stories concerning it.

The best way to assist your client through this fallout stage is to work with its personnel to formulate a list of responses to questions that are likely to come in, and to coach those individuals designated to handle these inquiries. Depending upon the size and scope of the breach, your client may wish to proactively approach publicity issues by working with a crisis management professional to create and deliver a press release and to assist in dealing with media and public inquiries.

If regulators contact your client, those inquiries should be directed to you as the outside lawyer. State attorney generals, the Federal Trade Commission or other consumer protection bodies may want to investigate the incident and your client's response to it. As the company's lawyer, you should take charge of the communications with all regulators.

Private claims brought by affected people may materialize, as well. Most state law data breach response statutes do not provide for a private right of action, but a few do, and consumers have filed class actions based upon common law theories of negligence and unjust enrichment, among others.

Data breach response is a specialized area of legal practice that is fraught with potential pitfalls for practitioners who are unfamiliar with the patchwork of often inconsistent state laws that largely control these incidents, or for practitioners who have not experienced the post-notification aftermath of responding to inquiries, investigations and claims. Every step in the data breach notification process should be taken with an eye toward minimizing later exposure and reputational harm to your client. "Dabbling" in data breach response counseling is not recommended. ■

Sandy Garfinkel is the chair of the Data Security & Privacy Practice Group at the law firm of Eckert Seamans Cherin & Mellott, LLC. He specializes in assisting companies and organizations in responding to breaches of data security, as well as incident planning and preparation. In the course of his practice, Garfinkel has handled a variety of types of data security incidents for clients within a number of different industries, including hospitality, retail sales (including Internet sales), manufacturing, energy, education and insurance, among others. He has written several published articles on data security issues, including "Anatomy of a Hotel Breach" (Hospitality Lawyer, June 2014), and is a frequent lecturer and writer concerning data security issues. He received his J.D. from Duquesne University and his B.A. from Emory University.