The Legal Intelligencer
THE OLDEST LAW JOURNAL IN THE UNITED STATES 1843-2015
THURSDAY, MARCH 5, 2015
An ALM Publication

E-DISCOVERY AND CYBERSECURITY

A Company's Data Breach Obligations: The Anthem Example

BY JANA LANDON

Maksim Kabakou/Fotolia

In early February, Anthem Inc.'s chief executive officer, Joseph Swedish, posted an extraordinary document. It was a detailed letter directed to Anthem members describing a cyberattack that exposed the personal information of approximately 80 million customers and employees, making it, according to The Wall Street Journal, likely the largest data breach disclosed by a health care company. In an all-too-familiar refrain, Swedish let consumers know that Anthem was working diligently with federal officials, that Anthem knew what information had been taken (and what information had not been touched) and that credit monitoring services would be available.

But did Anthem act too quickly?

There is a strong desire in most companies after a data breach occurs to begin remedial action, including notification of consumers, immediately. This has become particularly true after criticism was thrown at companies such as Home Depot and JPMorgan in the wake of their respective breaches. A company's desire to get out in front of these issues, however, must be tempered with consideration of its past history with breaches, its reporting requirements, and its internal preparation to handle the inevitable inquiries and lawsuits. In short, the current cybersecurity environment makes it evident that companies large and small must have a robust risk management plan that incorporates careful consideration as to when and how to report a breach so the company is in the driver's seat.

Following are a few steps a company and its counsel must consider before and after a data breach:

Have a Plan

One of the best steps any company, regardless of size, can take is to identify its potential data targets and create a comprehensive data breach plan with the assistance of counsel and information technology consultants. This plan should cover all aspects of an anticipated response, including investigation, preservation of data and notification. It should name specific contacts for legal issues, public relations issues and security issues. Having this type of plan in place will greatly reduce response time should a data breach occur. The company should also consider preparedness training for key members of the team to make sure that the plan can be put into action.

Preserve Data With Potential Litigation in Mind

For counsel, preserving evidence related to a breach may be one of the most challenging tasks. In the days following a data breach, the company is focused on remediating the issue, not preserving data—data that may be crucial in future litigation. A company must document what appropriate steps were taken to preserve information when the breach was discovered and document all actions taken in connection with, and in response to, an incident. Having a point person whose

only task is to document these steps is an important part of a risk management plan.

Given the lawsuits that arise from data breaches, the importance of data preservation cannot be overstated. Cases have already been filed against Anthem in California, Colorado, Florida, Indiana and Alabama, and will likely center on the security the company had in place before the breach and the steps it took upon discovery of the breach.

Engage IT Specialist and Outside Counsel

Many companies will find it helpful to engage an IT specialist and an outside law firm to assist with the investigation of a breach. First, it will be unclear at the outset whether anyone in the company was involved with the breach, either by inadvertence (e.g., not following security protocols) or through intentional behavior. Engaging competent counsel and vendors familiar with this type of charged environment is paramount. Second, an investigation takes time and resources that might not be available internally, thereby delaying a company's ability to quickly respond to breach issues. Third, security professionals and attorneys who deal with data breaches on a day-to-day basis may be able to offer insight that is unavailable internally. Finally, if the investigation is conducted internally without engaging counsel, the results of the investigation might not be protected by the attorney-client privilege or the attorney work product doctrine.

Notify Law Enforcement, Agencies and Individuals

To make sure a company has a full understanding of which laws apply to it, an attorney should be involved to assess whether the company is required to give notice in all states or countries where it does business or where data may have been lost. Note that this does not refer simply to the state or country in which a company has its headquarters; counsel must consider all locations where documents and data are stored.

Outside counsel can also help determine the form of the notice and, particularly, when the notice should be given. This is not an easy task, as it involves considerations as to whether the company's internal systems are ready to handle the onslaught of inquiries from the media, consumers and law enforcement. Any attorney providing advice should clearly document such advice.

Anthem receives mixed reviews on this point. Several data security sites and news outlets have written that Anthem's transparent and proactive response—only a few days after the breach was discovered—could signal a change in how companies protect their customers. Further, the FBI has praised Anthem for the speed in which it notified the authorities. Anthem's reporting deadlines, however, were likely much longer than a few days; federal law, for example, requires health care companies to notify regulators and consumers within 60 days. Because of its early announcement, many of Anthem's clients still have not been contacted, despite a promise that Anthem would "individually notify current and former members whose information [had] been accessed." Moreover, the website set up for questions regarding the breach (www.anthemfacts.com) does not even give the most basic statistics. This lack of concrete information is an indication that Anthem may have moved too soon, without having a plan for the inevitable backlash.

Learn From Past Breaches

Finally, no data breach plan should be static. Cybersecurity issues are moving at a rapid pace, and companies and their counsel must revisit the plan frequently to make sure it accounts for new company acquisitions, changes in technology and new risks. IT professionals for specific industries (including health care) often share information in order to combat attacks.

Anthem was very aware that potential risks existed and did exactly what many experts suggest: It reached out in various forums to share information. Specifically, it had been sharing information about the attacks with two key industry groups: Health Information Trust Alliance and the National Health Information Sharing and Analysis Center. Despite having been fined in 2013 over subpar security practices, however, Anthem did not encrypt the data on its system. Although the Health Insurance Portability and Accountability Act (HIPAA) does not require that such information be encrypted, it is very possible that Anthem knew it was a target and that further measures could have been taken.

Any data breach response must be carefully considered, as the response might impact not only the investigation and remediation of the breach, but also future litigation. A company should be sure that its response team is in place, that it has clear guidance, and that it is supported by experienced IT and legal professionals. The surge in security events over the past few months has made it evident that a data breach plan is an essential part of any company's risk management arsenal. •

Jana Landon *is counsel in Stradley Ronon Stevens & Young's Philadelphia office and co-founder and chair of the firm's e-discovery team. Her practice focuses on advising lawyers and clients on legal, technical and strategic issues regarding electronic discovery and information governance, as well as representing clients in complex insurance coverage and products liability matters. She can be reached at jlandon@stradley.com or 215-564-8049.*