NEWMEYER & DILLION LLP

CYBERSECURITY AND THIRD-PARTY VENDORS - ARE YOU ADEQUATELY PROTECTED?

By: J. Kyle Janecek

June 19, 2019

J. Kyle Janecek
Contact
949.271.7128
kyle.janecek@ndlf.com

Practice Areas
Privacy & Data Security
Business Transactions
Corporate Matters
Lending & Finance
Real Estate Transactions

There is an old saying commonly attributed to Napoleon Bonaparte, "what one should really fear is not a competent enemy, but an incompetent ally." While this has held true over time in a military context, it remains painfully true as applied to data security. Recently, two more entities, Quest Diagnostics and LabCorp, have learned this lesson. They join other targets such as Best Buy, Sears, Delta, Target and Chili's in learning that in the interconnected digital economy, all it takes is one weak link to create the opportunity for a data breach. Naturally, this leaves a question – what happens next? When the third party's data protection has failed and the breach has gone public, it may not be readily clear who is responsible for making the customers, and the entity whose data was lost, whole. A failure to account for what comes after risks being held liable for the breach, both legally and in the court of public opinion.

What Happened to Quest Diagnostics and LabCorp?

Quest Diagnostics and LabCorp both recently suffered a breach due to a vulnerability in a third party's data system. Both entities used a third party, the American Medical Collection Agency (AMCA), in order to bill and collect payments from patients. While specifics regarding the breach have not been disclosed as of yet, the breach has exposed credit card information, names, date of birth, phone numbers and other crucial information for millions of patients. Learn more in our most recent alert highlighting this breach.

This has sparked investigations and class action lawsuits against Quest Diagnostics and LabCorp in a variety of jurisdictions, with more likely to arise in the near future.

What Can You Do to Limit Liability Arising from the Actions (or inactions) of Third-Party Vendors?

Regarding third-parties, there are four main ways to curtail liability: (1) awareness of your organization's own data flow; (2) creating contractual protections; (3) requiring compliance with established standards; and (4) ensuring that the third-parties adhere to all applicable laws.

1. The first step is being aware of your organization's data flow – both when data is under your company's control, as well as when a third-party possesses the same data. Just as many businesses hire specialists to employ methods to track physical products from base materials to store shelves to determine the most efficient, secure way to create a profit, the same mentality applies to data. When planning to engage a contractor, the hiring organization should list, for its own reference, exactly how it receives the data from the consumer in the first place, what kind of data it receives, how the data is handled and how much data will be shared with the vendor – as well as the reason for sharing the data. Knowing if an entity is going to be processing crucial information, like payment information or social security numbers, will better inform what kind of safeguards need to be taken (i.e. contractual safeguards or insurance). If multiple contractors are used, then flowcharts, or similar pieces of information, can help speed along estimates of damage if a breach were to occur.

2. The second step is creating contractual solutions. An organization should consider various

contractual obligations to limit their own risks in using a contractor, in addition to completing due diligence on the contractor's security system and track record of cybersecurity incidents. The contractual requirements may include:

a. Requiring that the contractor allow your company to audit the vendor's security systems;
b. Require the contractor has insurance regarding any data breach (and name your company as an additional insured);
c. Ensure strong indemnification language that protected the organization against harm resulting from a security breach;
d. Require regular penetration testing; or
e. Place specific restrictions on the ways that the contractor may collect, keep or use the data.

3. The third step is requiring vendors to adhere to well-recognized standards. These should also be incorporated into the contract. The purpose of setting standards is to give a contractor something tangible and attainable to aim towards as a security measure. For example, a vendor might be required to be in compliance with the NIST or ISO 27001 standards. Or, a company may choose to require that, following any penetration tests, the contractor implements a patch in three days. Similarly, an organization can require that contractors encrypt data, and engage in cybersecurity training for their employees at least three times a year. There are a plethora of options – but requiring adherence to an established cybersecurity framework will help protect data and limit liability.

4. The final step is simply ensuring that your company, as well as outside vendors, adhere to all the applicable laws. The GDPR, Privacy Shield, and the new California Consumer Privacy Act (CCPA) all implement requirements on an organization to police its third party vendors. This effectively boils down to self-policing and ensuring that any contractor is aware of, and following, the requirements set forth in the agreement between the organization and vendor.

A Final Reminder

While an organization can do everything in its power to safeguard its data, and the data that consumers provide to it, there is no panacea. Third parties can help increase security, or they may increase risk due to lackluster cyber security practices. While this does not mean that a consumer will be blameless, or that the contractor will magically become liable for everything, it does mean that the additional link in the supply chain must be accounted for and secured, as that link may very well be the marginal difference in avoiding a breach.

Securing your organization's data will *always* be a complicated affair, and ultimately is an exercise in risk management. Security will likely never be perfect, but it can be attainable by intelligently balancing risks and preparing for the worst.

Kyle Janecek is an associate in the firm's Privacy & Data Security practice, and supports the team in advising clients on cyber related matters, including policies and procedures that can protect their day-to-day operations. For more information on how Kyle can help, contact him at kyle.janecek@ndlf.com.

ABOUT NEWMEYER & DILLION LLP

For almost 35 years, Newmeyer & Dillion has delivered creative and outstanding legal solutions and trial results for a wide array of clients. With over 70 attorneys practicing in all aspects of business law, privacy & data security, employment, real estate, construction, insurance law and trial work, Newmeyer & Dillion delivers legal services tailored to meet each client's needs. Headquartered in Newport Beach, California, with offices in Walnut Creek, California and Las Vegas, Nevada, Newmeyer & Dillion attorneys are recognized by *The Best Lawyers in America©*, and *Super Lawyers* as top tier and some of the best lawyers in California, and have been given *Martindale-Hubbell Peer Review's AV Preeminent®* highest rating.

For additional information, call 949.854.7000 or visit www.ndlf.com.