LOS ANGELES & SAN FRANCISCO
Daily Journal
www.dailyjournal.com
MONDAY, SEPTEMBER 27, 2021

PERSPECTIVE

Companies vulnerable to data breaches are now vulnerable to litigation

By Peter S. Selvin

Data breaches by large companies have been in the news for some time. Over the last several years several companies, including Marriott, Yahoo and Volkswagen, have been victimized by hackers who have broken into a company's computer network. In some cases, the hackers have put the company's confidential information on the internet. In other cases, the hackers have held the company's information hostage through ransomware.

While companies are rightly concerned about the security of their own networks, there is another risk. Recent court cases are testing the liability of companies and their directors for data breaches suffered by their vendors or service providers.

This is not surprising because companies often need to share confidential information with their vendors or service providers. An example that comes immediately to mind is where a company outsources its payroll management to an outside vendor. In that case, the payroll vendor will necessarily have the names, Social Security numbers and other private information of the company's employees. If the payroll vendor suffers a data breach, this private information may be disseminated, causing harm to the company's employees.

In such a case, it is a virtual certainty that lawsuits will not only be filed against the payroll vendor but also against the company itself. In those cases, the legal claim will be principally based on negligence — the concept that the company did not take due care in selecting the vendor or monitoring the vendor's computer network security system.

A recent case in Delaware took this a step further. *Laboratory Corportion of America Holding,* 2020-0305-PAF, (Delaware Chancery Court, April 28, 2020). In that case Laboratory Corporation of America contracted with a vendor to assist it in connection with the collection of past due accounts. The vendor suffered a data breach which resulted in the disclosure of the private health and financial information of over 10 million LCA patients. As a result, LCA was subject to a class action on behalf of a class of patients whose personal information was compromised because of the data breach.

But LCA's legal jeopardy did not end there. Following the filing of the class action suit, a shareholder of LCA brought an action against the company's directors. In his suit, the shareholder asserted that LCA's directors had allowed the company to provide personal healthcare and financial information to a vendor with deficient cybersecurity and data breach detection. The shareholder also asserted that the directors had failed to ensure that the vendor utilized proper cybersecurity safeguards to adequately secure patient information.

These liability risks mean that companies must not only focus on their own cybersecurity and data breach safeguards, but they must also be concerned about these safeguards in respect to their own vendors. The following are some risk-management ideas:

- Check that the definition of "insured computer network" in your own cyber insurance policy includes the networks of your vendors and your other service providers. By doing this, you will potentially have protection under your own insurance program for damage claims arising from data breaches that are suffered by your vendors or other service providers.
- Ensure that you have cyber insurance and that you carry sufficient limits under that insurance policy. This means that the amount of insurance available under that policy will be sufficient to protect the company in the event of a data breach incident.
- Make sure your vendor or other service provider carries its own cyber insurance policy with sufficient limits and that your company is named as an additional insured under that policy. The vendor's obligation to carry such insurance, and your entitlement to be named as an additional insured under that policy, should be expressly set out in the written agreement between your company and the vendor or other service provider.
- Require a written agreement between the company and the vendor or other service provider that, among other things, obligates those parties to defend and indemnify the company from any claims arising from a data breach suffered by those parties that result in a disclosure of the company's or the company's employees' private or confidential information. This indemnification obligation should be backed up by the vendor's or service provider's own cyber insurance policy that has limits sufficient to support that indemnification obligation. This written agreement also ought to give the company the right to conduct periodic audits of the vendor's or service provider's cyber security safeguards.
- Conduct regular cyber security audits of the vendor or other service provider to insure that proper safeguards are in place.

Liability for a data breach involving a company's or its employees' confidential information cannot be shifted by contract. Because a company runs the risk that it will be sued if its third-party vendor or service provider experiences a data breach, it should implement the risk management techniques that are described above. ■

Peter Selvin *is chair of the Insurance Coverage and Recovery Department at Ervin Cohen & Jessup LLP.*