Published on *The National Law Review* https://natlawreview.com

Fall-Out from Blackbaud Ransomware Attack

Article By:

Linn F. Freedman

As a follow-up to last week's post on the importance of due diligence regarding high-risk vendors' security practices, Blackbaud, a global company providing financial and fundraising technology to not-for-profit entities, notified its customers late last week that it was the victim of a ransomware attack in mid-May. Blackbaud offers a number of products to its customers, including aggregating research data of publicly available information on the wealth of individuals for not-for-profits to assess donors' giving capacity.

Blackbaud admitted that the ransomware attackers did get access to donor data and were able to remove a copy of a subset of data from Blackbaud's hosted environment. It has further stated that it paid an undisclosed amount to the ransomware attackers and received a certificate of destruction from the attackers. Blackbaud has stated that no sensitive information, including donors' Social Security numbers, credit card information or bank account information, was accessed or exfiltrated. According to a company spokesman, "[W]hile this sophisticated ransomware attack happened, we were able to shut it down and have no reason to believe this will result in any public disclosure of any of our customers' data."

Nonetheless, multitudes of not-for-profits have received notification of the incident and are struggling with how to respond. The responses have been anything but uniform. In addition, not-for-profit health care entities may have different legal requirements than other not-for-profits because of the Health Information Portability and Accountability Act (HIPAA).

The incident illustrated several things to consider:

- Do you have a vendor management program in place?
- Have you vetted or completed due diligence on your vendors' security practices?
- Do you have up-to-date and accurate contracts with your vendors, including a Business Associate Agreement, as applicable?
- Do you have contractual language in place with your vendors concerning appropriate data security measures to protect your data, what happens following a security incident, notification and indemnification?

- What are your reporting/notification obligations if one of your vendors experiences a data security incident?

- Who can help navigate these questions?

Mapping vendors that have access to data of your employees or customers is the first step in a vendor management program. This incident is a reminder that vendors are getting attacked just like your organization is.Your company data is your responsibility, even if it is in the possession of a vendor, so prioritizing your vendor management program may be worth consideration.

National Law Review, Volume X, Number 205