FPLG
FOR PURPOSE LAW GROUP
A Professional Law Corporation

GENERAL

After Blackbaud: More About Nonprofits & Cyber Security

11.12.20 | Linda J. Rosenthal, JD

When the news broke in July 2020 about the massive security breach against Blackbaud, perhaps the nonprofit sector's leading provider of cloud-based data-management services, there was immediate alarm. By late September, fuller – and more disturbing – details emerged.

We wrote about it in *Blackbaud Data Breach: Fallout for Nonprofits* (September 29, 2020). The intrusion has been described as a series of classic "pfishing" maneuvers that grabbed the data supplied by nonprofits primarily from around the U.S. and the United Kingdom. It was followed up by the standard "ransom" demand for payment by Blackbaud to return the stolen data.

If the computer breach itself weren't bad enough, Blackbaud's handling of the mess compounded it exponentially. The data giant failed to discover it for at least three months in the spring of 2020, quietly paid an unknown amount of ransom in return for as-yet-unverifiable promises and representations by the cyber criminals, and did not disclose any of it until mid-July.

As more details seeped out in the following weeks, there were more questions than answers. By late-September, nonprofit clients had filed at least ten lawsuits for negligence, invasion of privacy, and breach of contract, among other claims. In particular, the plaintiffs allege that "… the company's assurances that the hackers destroyed the information they stole is not reasonable." They assert that "… as a result of the data breach, plaintiffs and thousands of other class member users suffered ascertainable losses in the form of out-of-pocket expenses and the value of their time reasonably incurred to remedy or mitigate the effects of the attack."

And now the legal jeopardy is spilling over to the nonprofit clients, which have contractual and statutory duties to their own end users whose personal data got mixed up in this mess. The title of a September 25, 2020, article by editor-in-chief Ruth Cambridge in *The Nonprofit Quarterly* aptly sums up this predicament: *Lawsuits Proliferate in Blackbaud Incident: Nonprofits, Consult Your Lawyers*.

Steps for Blackbaud Nonprofit Clients

Even in the midst of a catastrophic pandemic, nonprofits must be vigilant about the ever-present risk of cyber attacks. That responsibility is challenging enough without the added layer of complexity with the Blackbaud situation; that is, being in the middle of the chain of intrusion.

For Blackbaud clients, there are serious, immediate issues and concerns. "There are '… multitudes of not-for-profits [that] have received notification of the incident [but] are struggling with how to respond. The responses have been anything but uniform.'" On top of the breach itself, the "delays of several months have made the position of the nonprofit client that much more precarious."

Among the many experts contributing advice to nonprofits on how to proceed is Allison Ward Davis of CapinCrouse LLP in *Steps to Take After the Blackbaud Breach* (August 7, 2020). For Blackbaud clients, a threshold issue is evaluating the "…real impact on" them. This inquiry will likely evolve as the weeks and months go by and more information is available. The steps that Ms. Davis recommended back in early August include:

- Determining the extent of your organization's exposure including which records were involved.
- Evaluating and clarifying Blackbaud's actions and responses.
- Determining if you must notify your affected constituents, clients, beneficiaries whose data was stolen. "Depending on where your organization is located and what privacy laws and regulations apply, there may be breach notification requirements if specific information was compromised. Many organizations are choosing to err on the side of transparency and openness with their constituents and are notifying their affected donors regardless of mandated requirements."
- Consider "forcing a password reset and enabling multi-factor authentication (MFA)." Also, "revisit your application settings." In that regard, Ms. Ward links to several of her earlier blog posts: *Application Security: Understanding the Risks* (Part 1) (February 14, 2020) Allison Ward Davis, *CapinCrouse LLP Blog; Application Security: Recommendations and Next Steps* (Part 2) (February 14, 2020) Allison Davis Ward, *CapinCrouse LLP Blog*
- Evaluate how well Blackbaud is doing to reduce a future breach and whether the toolkit and other resources they have provided are adequate.
- Request a "periodic local backup copy of your data."

Cyber Security Reviews: All Nonprofits

"The Blackbaud breach," Ms. Davis reminds us, "is not an anomaly. Reputable vendors are targeted all the time, and unfortunately, some of these attacks are successful and can affect your organization."

All nonprofits should "proactively plan for vendor issues" to reduce the impact of a future breach. She recommends these steps:

- "Establish vendor management processes." This will help you evaluate whether a prospective (or existing) data-storage firm is able to adequately protect your data. It also helps you prove to your own clients and beneficiaries that you exhibited "due care" and "due diligence."

- "Ensure vendor controls contain critical IT stipulations." A contract for data storage should clearly spell out the data firm's "responsiblity for confidentiality, information security of your data, and breach notification in the event an incident occurs."
- "Establish a data inventory." Creating and maintaining this information will enable you to rapidly assess the impact of a breach of your vendor's security.
- Make a plan to assess vendor incidents. An organization may already have an "incident response plan" but generally they focus on internal cyber attacks. The massive Blackbaud breach brings into clear focus the necessity of including the intrusion of a vendor's data into the scope of advance planning. In any event, it's critical for nonprofits to review and reinforce their own existing internal controls and preparations. "If a large vendor can become a victim, so can you!" These steps include having "strong application settings" – [see resources above] – and establishing retention periods for data in vendor systems to minimize the impact of a breach." Also, make sure you retain "periodic local backups of your hosted data."
- Keep up-to-date on the data privacy laws that apply to your organization. "Many laws have timeframes for notification and if you don't know these before the issue happens, you may not be able to comply."

Conclusion

Since our post in November 2016, *Nonprofits And Cybersecurity: Make It A Priority*, we've revisited this important topic several times because of the "pervasiveness of the threat of cyber attacks, and the catastrophic amount of damage that invariably follows a computer breach."

The Blackbaud breach brings into sharper focus the breadth and scope of that threat, and calls for immediate reviews and action by all nonprofit organizations

— Linda J. Rosenthal, J.D., FPLG Information & Research Director