More Than Money: Data, Fundraising, and Your Nonprofit

Scenario: Whitebaud Data Breach

At 9 am this morning, NY Food Bank found out that data about their employees, donors, and other stakeholders stored in their fundraising software was hacked. The hack was not a direct hit on their own network but a breach of their provider, Whitebaud, as part of a larger ransomware threat.

215 of NY Food Bank's nonprofit partners are now at risk because of the breach, as well as all of their donors. Admittedly, NY Food Bank is not alone: Human Rights Watch, Planned Parenthood, and NPR have confirmed that they are victims of the same breach at Whitebaud.

What NY Food Bank CEO Thao Nyugen is most angry about is that the attack happened on February 7th but went undetected until May 14th, and they were not notified until July 15th. When notified, her org was not given answers as to how the breach happened or what would be done to protect data in the future, but was merely directed to a list of online resources.

In an official statement by Whitebaud's chief technology officer, John Doe, the company has since explained that there was a suspicious log-in on an internal server on May 14th. This entrance allowed the cybercriminal to access a data center server, but they did not get into its cloud operations. The criminal removed a copy of a subset of data from the desktop.

"The attack was sophisticated enough that it initially looked like legitimate customer activity. When it escalated, the attack evaded our endpoint detection, intrusion prevention, and monitoring processes," an official explained. It was eventually tracked back to the February date.

The cybercriminal was in frequent contact requesting a bitcoin ransom until June 18th.

Doe has assured people that no social security details, bank details, or other sensitive material was removed. It has become apparent that what was stolen was customer and product lists and a large amount of health information.

- What measures should NY Food Bank take to protect its stakeholders from future harm?
- What information should they release to partners that they suspect were impacted by the breach?

In addition to contemplating how to keep data safe from breaches in the future, the NY Food Bank is also considering its own liability to inform stakeholders, including donors and individuals registered

in their databases who may have been affected by the breach. There are many things to consider, including how to effectively notify stakeholders, given the lack of internet and device access within the community NY Food Bank serves. Data breach laws and regulations are complex and the organization feels out of their depth.

- Who should they call?
- Where can they look for information?
- How can they notify their stakeholders without eroding trust and who should be held accountable?
- What contractual clauses in their vendor relationship with Whitebaud have been flagged by NY Food Bank's lawyers?
- Does it make any sense for NY Food Bank to try to organize other Whitebaud clients in response? What might they do together?