Lessons Learned from Data Breaches

By Chris Purnell, Partner and Tax Counsel, CapinCrouse, and Allison Davis Ward, Partner, CapinTech

Recently, a company that provides hosting of a cloud-based nonprofit software had a breach that resulted in the compromise of the donor and contact information of numerous organizations. With more and more data breaches happening, organizations are determining how to best address the issue and move forward.

All nonprofits are at risk of being impacted by a data breach at their organization or a key vendor. And in the wake of a breach, there are numerous audit, tax, and cybersecurity considerations. In this article, we'll address some of those considerations and steps you can take to better prepare your organization for the future, whether or not you were affected by this or other recent breaches.

Audit and Tax Implications

After a cyber breach affects a nonprofit, it is common for donors and other constituents to request that the nonprofit no longer house their data. As we detail in the Regulatory and Cybersecurity Implications section below, this is a right afforded to constituents under various regulations. However, in addition to meeting the regulations, if your nonprofit receives these requests, you also need to ensure that you have the necessary data to perform some fundamental tasks related to audit and tax requirements.

This includes:

- **Providing contemporaneous, written acknowledgment of contributions.** If donors wish to deduct a charitable contribution of any amount, they will need to substantiate that contribution. However, if donors wish to deduct a charitable contribution valued at $250 or more, they will need a contemporaneous, written acknowledgment of the contribution from the nonprofit. This acknowledgment must contain:
  - The name of the organization;
  - The amount of the contribution;
  - A description of the value of any non-cash contribution; and
  - A quid pro quo statement noting either that no goods or services were given in exchange for the contribution (other than intangible religious benefits) or, alternatively, the value of any goods or services that were given to the donor.

  By necessity, your organization will need to maintain some basic information to generate this contemporaneous, written acknowledgment.

- **Meeting donor restrictions.** If a donor has placed any specific restrictions on a contribution, your organization will need to keep a record of these to ensure that you meet the donor restrictions appropriately and release the contribution when the purpose or time restriction has been met. This is especially true if the restriction will apply for a significant period of time. And for contributions with a permanent restriction in place, it is very important to retain documentation of the donor's intent. These factors are important to consider with respect to accurate financial reporting and retaining adequate supporting documentation that your independent auditors may request during audit procedures.

- **Providing financial statement disclosures.** Disclosure of the concentration of donations by significant donors and related-party disclosures are required for nonprofit financial statements. This means your organization needs to retain adequate records to ensure that the proper footnote disclosures can be made to support the financial statement presentation.

In the wake of a breach, there are numerous audit, tax, and cybersecurity considerations.

- **Recording donor preferences.** At many deputized fundraising organizations (such as campus ministries and international mission organizations), it is imperative to keep very clear and up-to-date records on which missionary or staff person a donor has chosen or prefers to support. While the decision on how the funds will be used is at the sole discretion of the nonprofit, it is understood that the nonprofit will strongly consider the donor's choice.

The IRS also has several key interests in nonprofits maintaining donor data. If your organization files a Form 990, you may be required to file a Schedule B to the form. This is a list of contributors who have given more than a certain amount to the nonprofit during the prior fiscal year. Information on how much was contributed, as well as the donor's address, is necessary to complete Schedule B.

Further, if your organization is a public charity under the public support test, you will need to maintain information about the amount of donor contributions in order to demonstrate that you still qualify under the public support test. The public support test requires that a public charity receive 33.3% of its funding from "public sources," or receive 10% from public sources and satisfy a facts and circumstances test. Since this is a five-year calculation, the nonprofit should keep the contribution data for at least that long. This five-year period also covers the normal timeframe for an IRS audit of Form 990, which is generally three years from the filing date.

Practical Suggestions

Certain donors may request that their data be purged from all electronic records. To facilitate this request, your organization could move the donor contributions to an "anonymous" category and delete the pertinent donor information. This would ensure that the subsidiary donor records would still reconcile to the general ledger contribution accounts. However, in this situation, it would be important for your organization to retain sufficient hard copy records of the details of the "anonymous" category to support the required financial statement disclosures and IRS requirements noted above.

Your organization should also review your document retention and destruction policy to see if it has provisions for when someone requests that their information be deleted. If the policy does not address that particular issue, you should consider updating and revising the policy to ensure a consistent response from your organization.

Regulatory and Cybersecurity Implications

Depending on where your organization operates, there may be relevant laws and regulations that impact your response to a breach. For example, if you operate in the European Union, you may be subject to the General Data Protection Regulation (GDPR). And in the United States, laws and regulations vary at the state level and each has different requirements.

As a result, there may be different requirements related to constituent rights and notification based on where your constituents are located and where they were when you collected their information.

We recommend that you work with legal counsel who is fluent in these matters to determine your legal requirements related to breach notification and constituent rights. Regardless of what is required by the various laws, you may decide to err on the side of transparency and openness with your constituents.

In addition to notifying constituents of a compromise of their information, many constituents may contact you to request that their information be removed from your systems. This is often known as the "right to erasure" or the "right to be forgotten," and this is a right afforded to constituents under various regulations, including GDPR.

Certain rights like this can present unique challenges. First, it can be very difficult to know all the places where constituent data may be stored, and the openness to interpretation of some of these laws can make it challenging to know what is actually required. For example, constituent records are often not backed up in a single file independent from other constituents. Therefore, it may be extremely difficult for an organization to purge a single constituent record from the backups of its databases without impacting the backups of the other constituent records.

Again, your legal counsel can advise you in these matters, but there may be exceptions to various rights in instances where addressing the right is not technically possible, prohibitively expensive, or certain data is legally required to be maintained. And as we noted above, nonprofits also need to retain certain information

We recommend that you work with legal counsel who is fluent in these matters to determine your legal requirements related to breach notification and constituent rights.

for audit and tax purposes. Discussing these exceptions with your legal counsel, maintaining appropriate documentation of the exceptions, notifying your constituents about what is being done to address their request, and revisiting the exceptions to address them when feasible can support your due diligence to meet the requirements under these laws. It is important to remember that for many of these laws and regulations, there is a time requirement for notifying the impacted individuals or responding to requests related to specific rights, such as the right to be forgotten. So if you haven't already discussed this area with your legal counsel, you should prioritize this discussion to ensure you respond appropriately.

Finally, many companies purchase cybersecurity insurance to help them offset the impact of a breach. That coverage often provides access to various specialists that the insurance company recommends you consult with, including attorneys who focus on cybersecurity matters. However, mission-based organizations often have unique concerns related to their mission and the donors that support them and may choose to engage their own resources to help navigate some of those considerations. If you do this, it is imperative that you discuss with your insurance company any actions you plan to take to ensure you do not act against the stipulations in your policy and invalidate your ability to make a claim.

Reevaluating risks and your mitigating controls periodically can help you identify areas where additional protections may be warranted.

Next Steps

Once the aftermath of a breach has settled, there are many steps you can take to be better prepared in the future.

- **Discuss lessons learned with your vendor.** Ask your vendor what actions have been taken to reduce the risk of a similar breach happening in the future. No organization is immune to incidents, and there is no cure-all control; however, ensuring that your vendor is taking proper steps to remedy issues is a key component of ongoing due diligence.

- **Establish processes for ongoing vendor management.** Reviewing your vendors' controls for security, business continuity, disaster recovery, and incident response can provide continued assurance that they have the means to protect your data. Similarly, strong vendor management oversight shows that your organization is exhibiting due care.

- **Ensure vendor contracts contain critical IT stipulations.** Contracts should define the vendor's responsibility for confidentiality, information security of your data, and breach notification in the event an incident occurs.

- **Create and maintain a data inventory.** Without knowing where your data is, who accesses it, how it is stored, and where it is transferred, you may not know the full impact of an incident. Maintaining this inventory will help you quickly assess the impact of an issue.

- **Develop a plan to evaluate incidents at vendor locations.** Ensure your Incident Response Plan defines vendor issues as incidents to be investigated. Many incident response plans focus only on internal attacks, but incidents at vendor locations affect you and your constituents and should be considered.

- **Evaluate breach and privacy laws.** Proactively investigating and knowing which data privacy laws apply to your organization ensures that you can respond faster. Many laws have timeframes for notification and if you don't know these before the issue happens, you may not be able to comply.

- **Enhance internal preparations.** Think about what you can do internally. If a large vendor can become a victim, so can you! Reevaluating risks and your mitigating controls periodically can help you identify areas where additional protections may be warranted.

Please do not hesitate to contact us with any questions about this or other audit, tax, or cybersecurity issues. We are here to help.

About the Authors

Chris Purnell, Partner
Tax Counsel
CapinCrouse
cpurnell@capincrouse.com
o 505.50.CAPIN ext. 1113

A licensed attorney, Chris advises exempt organizations of all sizes on a wide range of issues, including tax and employee benefit related matters, representation before state and federal tax authorities, and assistance with firm audit or advisory engagements to formulate advice and counsel on important operating and tax issues. Chris also assists clients with general tax issues, unrelated business income, charitable solicitation, and missionary employment structures. Prior to joining CapinCrouse in 2019, Chris served as the Executive Director of the Neighborhood Christian Legal Clinic, one of the nation's largest Christian legal aid organizations.

Note: Although licensed to practice law in Indiana, Chris's services through CapinCrouse do not involve the practice of law and consequently do not result in the creation of an attorney-client relationship.

Allison Davis Ward, Partner
CapinTech
award@capincrouse.com
o 505.50.CAPIN ext. 2008

Throughout her time as an information systems auditor, manager, and partner, Allison has provided information security assessment and consulting services primarily for nonprofit organizations, financial institutions, and health facilities. In addition to these services, she has provided clients with consulting services in risk assessment and policy development engagements.

About CapinCrouse

As a national full-service CPA and consulting firm devoted to serving nonprofit organizations, CapinCrouse provides professional solutions to organizations whose outcomes are measured in lives changed. Since 1972, the firm has served domestic and international outreach organizations, universities and seminaries, foundations, media ministries, rescue missions, relief and development organizations, churches and denominations, and many others by providing support in the key areas of financial integrity and security. With a network of offices across the nation, CapinCrouse has the resources of a large firm and the personal touch of a local firm. Learn more at capincrouse.com.

CapinCrouse is an independent member of the BDO Alliance USA.

About CapinTech

CapinTech, a CapinCrouse company, provides information security services, including cybersecurity assessments, consulting, and training services, to financial institutions, nonprofit organizations, medical entities, professional services firms, and other organizations. Each year the firm performs hundreds of assessment, consulting, and speaking engagements with a team of experienced professionals retaining numerous certifications, including CPA, CISSP, CISM, CISA, CITP, CGMA, and CTGA. Each engagement is tailored to fit the unique needs of the organization, and information and reports are presented in a clear, concise manner intended for an audience with varying information systems (IS) knowledge. More information is available at capintech.com.