Nonprofits Are Not Immune to Maintaining Data Privacy

By Karen Schuler, CFE, IGP, IG[P]

It is 6 a.m. and you receive a call from your chief financial officer that your donor data has been stolen. What do you do? Whom do you call? How do you handle this situation? I find that a fair number of our nonprofit clients are unaware of where their data resides, who has access to it, and how it's protected. So, let's explore some methods that your organization can employ to better protect the privacy of your donor, employee and volunteer data. This is the first of two articles that will better prepare you to implement a data privacy program.

Step One

Understand Regulatory Standards

Due to the prevalence of data breaches, data privacy standards are popping up across the globe. Regardless of whether you operate in the United States or internationally, it is critical to understand which data privacy regulations apply to you. In the United States there are approximately 20 sector-specific national privacy or data security laws, and hundreds of them among the 50 states. From a global perspective, there are thousands of data privacy laws that have been in place or are coming into law in the next several months. Regardless of where you operate, you need to understand how your organization should comply.

Step Two

Identification

The next step is to ensure you understand what information you have and where it is. Certainly there are tools to assist with this, but if you do not have the budget to access those tools, start by conducting interviews of the individuals that manage certain types of applications and data. During these interviews, gain an understanding of what software applications or technology are used to conduct your business, identify where that data is stored, whether it's managed internally or externally, and how long data is retained.

To prepare your data inventory, follow these steps:

1. Obtain application inventories that might already exist.
2. Update the application inventories.
3. Gain an understanding of who manages each application.
4. Identify what types of data are stored within each application.
5. Understand how long certain data types are retained.
6. Determine where your most sensitive types of information reside.
7. For those critical sets of data, map how the data flows through the organization, who manages it, who has access to it, and where security gaps might exist.

Due to the prevalence of data breaches, data privacy standards are popping up across the globe.

Step Three

Classify Data

There will be certain types of data that you consider very sensitive while other types might be considered less critical or sensitive to the organization. To develop classification schemas, use a guide similar to the one outlined below.

Regardless of the size of your organization, classifying data is a critical step in protecting the privacy of your information.

Step Four

Align Policies with Data Classifications

Once you have classified your data, the next step in the process is to understand what data protection policies are currently in place and whether they are current or need updating. Often times an organization will find that its policies have not been updated for years. This can be more detrimental than not having policies at all. The key is, if you create policies, ensure there are good governance and management practices to maintain those policies. Typical policies that are essential to maintaining the privacy of data can include:

- Data classification
- Data retention
- Legal hold
- Data security
- Data handling
- Information lifecycle management
- Data privacy

As you are developing your policies, your technical or security teams should ensure that the information contained within each policy matches actual controls. In other words, it is critical to align your security practices with your policies.

Step Five

Implement and Train your Team Members

Once you complete the above steps, it's time to develop an implementation and change management strategy as well as a training program. Training and change management are critical to performing a successful roll out of any program. And, although implementation plans vary widely, standard steps that can be employed in any organization include:

- Pilot: Test the process, policies or procedures with a small group.
- Utilize Technology: Understand what technology can be utilized to better manage policies, procedures or processes over time.
- Roll-out: Once you conduct the pilot, begin to rollout the program to all team members.
- Training: Immediately following your roll-out or implementation step, ensure that each team member is trained in a timely manner.

Now that you have these steps under your belt, it is time to move on to establishing the privacy program. Stay tuned for a future article where we will provide you the steps needed to expand into a formal privacy program.

Guide to Classification of Data

Classification	Description	Examples
Public	This type of data may be disseminated to the public ***without potential harm*** to the organization or its constituents.	• Brochures • Advertisements • Job opening announcements • Press releases
Internal Use Only	This category of data means that exposure to the public ***could adversely impact*** the organization or its constituents.	• Financial records • Security documents • Workflow • Internal memos
Confidential	This category of data is to only be disseminated to those who ***need to know***.	• Contracts • Personnel matters • Internal business plans • Strategic plans
Restricted	This category of data ***would cause irreparable harm*** to the organization if it were to be disseminated to the public.	• Protected Health Information • Personally Identifiable Information • Intellectual Property • Donor lists • Dissolution documents

For more information, contact Karen Schuler, managing director, BDO Litigation and Forensic Technology Systems, at kschuler@bdo.com or email CapinCrouse at info@capincrouse.com.

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.

AN INDEPENDENT MEMBER OF BDO ALLIANCE USA

CapinCrouse is an independent member of the BDO Alliance USA.