Non-Profit Organizations Can Reduce Risks by Addressing Data Privacy Concerns in Advance

Description

With the threat of cyber-attacks making the news, it is a good time for all non-profit organizations to review their policies and procedures with respect to data privacy. Many non-profit organizations are particularly vulnerable to legal, financial, and reputational risks resulting from cyber-attacks and other data breaches because they do not have the staff, time, or resources to devote to understand and implement the myriad of laws that may apply to the organization. But there are rarely exemptions from these laws for small organizations or for non-profit organizations.

In addition to compliance obligations, the fallout from a data breach incident could be harmful or fatal to an organization. Many states have laws that may require notice to affected individuals, offering remediation such as free credit monitoring (the organization would have to pay) for a period of time, fines, and penalties. For example, a hospital in Massachusetts was fined $1.5 million after the theft of a laptop computer containing unencrypted health information of patients and research subjects. In addition, the organization could suffer reputational damage from the data breach, which may be worse than the financial damage.

In this day and age, organization leaders have no choice but to take the time to understand the risks that arise from collecting and storing personal information from employees, donors, volunteers, and clients. This article explores some of the issues that the organization should consider.

Identify the Data

The first step is to identify what data the organization possesses or controls and where the data resides, and to classify that data by risk. Various federal and state privacy regulations require that entities protect personally identifiable information (PII) no matter where it resides, and whether it is in paper or electronic form. A typical organization may have data stored on a network; on stand-alone systems such as billing, medical, donor, and marketing databases; on storage devices like thumb drives and CD's; on remote devices such as laptops or employee-owned cell phones and home computers; on paper; and with vendors and suppliers. Copies may be stored on backup devices or with a third-party service provider.

Classify the Data

There are many different ways to classify the data. One scheme is often used based on the potential risk of its use and disclosure. **Highly sensitive data** is data that is extremely important to the organization, and that could cause major or irreparable harm to the organization if disclosed or compromised. Examples of highly sensitive data include protected health information, personally identifiable information about employees, clients and other individuals, trade secrets, and donor lists. **Confidential data** is data that is not highly sensitive but is meant for internal use and still needs to be disclosed on a "need-to-know" basis. Disclosure of confidential data should not have major adverse effects on the organization. Examples of confidential data are non-public contracts, personnel hiring, termination and disciplinary decision, and confidential information regarding the organization, such as internal finances, strategic plans, and information and physical security plans of the organization. **Public data** is data that is that is not sensitive and is available to the public or that the organization disseminates. Examples of public data are the contents of the organization's website, marketing materials, and information in public reports and documents.

Create and Align Rules and Policies

Once the organization has identified and classified its data, the next step is to determine what policies are

currently in place to protect the data and whether the policies need updating, and what additional policies are needed to address gaps. Each policy should also have someone with the responsibility of reviewing the policy no less often than annually, and to update the policy as needed. There are many different types of policies that an organization could have, depending on its activities. But some of the more typical policies address password protection, use of employee devices for organization business (so called “bring your own device” or “BYOD” policies), retention and destruction of documents, access control to information (who can access what information), information security, physical security, employee privacy, donor privacy, telephone call and video call recording, verification of payments and wire transfers, responding to data breaches and other data security incidents, and use of social networking and email for the organization.

Develop a Written Information Security Program

Once the organization has developed its policies, it needs to put them together with an overall “Written Information Security Program,” commonly known as a “WISP.” If the organization has employees, customers, or donors in Massachusetts or Rhode Island, it must have a WISP. Many other states have similar requirements.

If the organization (wherever located) collects, stores, or uses personal information about an individual, many states have laws that legally require the organization to: (a) develop, implement, and maintain a comprehensive WISP; (b) implement physical, administrative, and extensive technical security controls, including the use of encryption; and (c) verify that any third-party service providers that have access to this personal information can protect the information. “Personal information” can be a first name, last name and the last 4 digits of a social security number, credit card number, or bank account number of a customer.

Organization leaders need to understand that the WISP is a “program,” not a “policy.” The WISP is intended to describe a system by which one runs the business on a day-to-day basis to safeguard sensitive information. Our experience with WISP’s is that some clients treat them like policies that they can have drafted and then throw in a drawer and never look at again. Some organizations have copied a WISP from a form found on the Internet, or a form provided by another company, but have not taken the time to customize it for their organization. Other companies want to say they have a WISP, but do not actually make any operational changes to implement the purported security programs described in the WISP. This practice can be risky under state laws, such as Massachusetts.

There are several reasons why it is important that all organizations prepare a WISP and update it regularly:

- WISPs help to reduce the risk of liability and adverse publicity should a data breach occur. State enforcement officials have pursued and obtained six figure civil judgments for violations of these regulations. In addition, the laws in some states require breach notices to state whether or not the company maintains a WISP;
- Some state laws, such as those in Massachusetts, require organizations to review their WISP’s at least annually. We see many companies who initially prepared information security programs but have not reviewed or updated their policies on a regular basis; and
- Information security programs help with training employees in company policies and procedures with respect to confidential and sensitive information.

Implementation and Training

The next step is to implement the policies and train the staff. New policies may require pilot testing and roll-out, while existing policies may not. All staff should be trained in all of the policies. In addition, training should be updated periodically. For example, some companies require employees to undergo annual cyber-security training.

Consider Cyber Insurance

Bringing an organization online introduces new risks, including the need to have more digital data about the organization's clients and donors, such as credit card information, names, addresses, contact information, and donor and service history. Some of that data may be stored on the organization's computers, and some may be stored with a third-party vendor in the "cloud."

All of this digital data is vulnerable to attacks by third parties who want to access it. Cyber-attacks can cause harm to an organization in a number of different ways. It will incur costs to investigate the cause of the attack and to recover data and systems and may be forced to pay a ransom fee to "unlock" the organization's data. In addition, after a cyber-attack occurs, the organization also may incur costs to investigate the breach, to notify customers and other third parties (such as regulators and attorneys general) if sensitive information is involved, and to defend and settle lawsuits involving claims that the organization did not act properly in protecting the data.

Many organizations are surprised to discover that their general commercial liability policies do not cover most types of cyber risks. Commercial general liability policies typically only cover bodily injury and property damage, not monetary losses, ransom costs, or regulatory fees and expenses. In addition, coverage is often limited to losses caused by "tangible" means. Insurance companies typically consider data breaches to be "intangible" causes not covered by the policy. Most commercial general liability policies also include an exclusion for access to or disclosure of confidential information, and the resulting liability.

One important tool to reduce the risk is a cyber insurance policy. There are many differences among policies, so it is important to discuss coverage with an insurance broker or agent with experience in this area.

Defending against cyber-attacks has become a cost of doing business for all organizations, not just large companies. The first defense is to have consistent policies and procedures in place that are followed by all employees and others who have access to confidential data. As a backstop, cyber insurance can be an important part of that defense for many organizations.

Date Created
May 20, 2022