Spring 2023

Profitable Solutions for Nonprofits

Is your cybersecurity up to snuff?

7 tasks for a successful nonprofit finance committee

Charge it!
Credit card issues for nonprofits

NEWSBYTES

LAPORTE
CPAs & BUSINESS ADVISORS

New Orleans | Houston | Baton Rouge | Covington | Houma
Check out our Nonprofit Industry Group page and nonprofit blog.
laporte.com/industry/nonprofit

Is your cybersecurity up to snuff?

The sudden and unexpected shift to remote work in 2020 made clear that many nonprofits have vulnerabilities that cybercriminals could leverage to steal data or disrupt operations. Your organization's employees may or may not be back in the office, but the risks are ongoing. Here's what you need to know about the most crucial components of effective cybersecurity for nonprofits.

Culture of security

When cybersecurity is recognized as a top priority throughout an organization, the odds of being victimized drop dramatically. It only takes one employee to click on a risky link in a phishing email (see "Know your cyberattacks," on page 3) or fail to update software to expose the entire organization. So you need everyone to be on board. Employees who see best practices routinely implemented are more likely to duplicate those practices and less likely to fall prey.

As with so many things, the tone starts at the top. If organizational leaders are exempt from measures required of others (for example, regular training or password protocols), employees notice and might take their own compliance less seriously. To create a pervasive commitment to cybersecurity, all policies, practices and procedures must apply to everyone.

Restricted access

You should grant data access solely on a "need-to-know" basis. Too many nonprofits allow access to employees or volunteers who don't actually require access to do their jobs. These people may all be trustworthy on their own, but each one represents an avenue to data that a cybercriminal could compromise.

In shared file systems, take advantage of permission settings to limit access, review permissions monthly or at least quarterly, and remember to shut off permissions when employees or volunteers are no longer with your organization. Require authorized users to use multifactor authentication and set up alerts for when these users are logging in from unfamiliar devices or unusual geographic areas.

Incident response planning

Even with comprehensive, up-to-date cybersecurity policies and tools, no organization is immune from cybercrimes. Formulating an incident response is essential to minimizing the repercussions of a successful attack. You don't want to be scrambling for the right response in the heat of the moment.

Consider establishing an incident response team (IRT) to develop a detailed written plan for handling attacks. Ideally, your IRT will be cross-disciplinary, with representatives from areas including management, IT, human resources, finance/accounting, marketing/communications, and member or client services. Each area should assume specific roles and responsibilities in the event of an attack. It's best to have two representatives from each area to improve the odds that someone will be available to respond if an incident occurs.

Annual risk assessments

Cybercriminals don't rest on their laurels — they're constantly ferreting out new vulnerabilities and devising new tactics for exploiting them. So don't assume the cybersecurity protections you put in place last year are still up to the task. Whether conducted by an internal IT employee or a third-party expert, your organization should undergo an annual cybersecurity risk assessment.

At the most basic level, every assessment should determine the data you currently possess and collect, how you store it, whether you truly need it, and how you dispose of it. In addition, identify all parties that have access to your data (for example, vendors) so you can evaluate whether they use appropriate security protection. Once you've determined the risks, weigh the likelihood of each risk actually occurring and the likely consequences. These evaluations can guide you in adopting additional steps to mitigate risk.

Assign responsibility

In today's environment of evolving risks, every nonprofit needs to formally assign responsibility for cybersecurity. If you lack the resources to employ a full-time cyberofficer on staff or your IT employees are overstretched, you might want to outsource the job. Balancing the upfront costs against the potential ramifications of a breach should make clear that you can't afford not to. ■

Whether conducted by an internal IT employee or a third-party expert, your organization should undergo an annual cybersecurity risk assessment.

Know your cyberattacks

You're not alone if you get confused by the various descriptions of cybercriminals' schemes. Here are some of the most relevant for nonprofits:

Phishing. This generally refers to schemes where cybercriminals trick victims into providing personal information (including login credentials) or clicking on links in emails or texts that infect computers with malware. Many iterations exist, with more emerging.

Malware. Malicious software encompasses a variety of viruses, including ransomware and spyware. It's often unleashed when an employee clicks on a phishing link, resulting in malware installation. Ransomware can block access to critical data and could shut down a system completely, requiring the organization to pay a ransom to regain access. Spyware allows the transfer of data to the criminals.

Denial-of-service (DOS) attack. DOS attackers overwhelm a victim's servers, networks or system, eating up their resources and bandwidth. As a result, servers and networks aren't available for their intended users. Visitors may not be able to reach the organization's website, or employees might be unable to do their work.

7 tasks for a successful nonprofit finance committee

A nonprofit's finance committee oversees and keeps its board of directors apprised of the organization's overall financial health. This should be more than simply scanning financial reports. An active finance committee is crucial to maintain a nonprofit's health and reputation. The success of your finance committee depends on your board, staff and committee members understanding the committee's duties.

Finance committee responsibilities

Although the exact parameters of committee member participation will vary based on factors such as staff size and organizational budget, the finance committee generally should be involved in the following:

1. Communicating with the board. The committee works with staff to determine the best way to convey information the board needs for sound decision-making. Not everyone understands financial statements and related jargon. Numbers require explanation and context; the committee must connect them to the organization's mission, goals and strategies.

2. Budgeting and financial planning. Before beginning the budgeting process, the committee should identify key assumptions and initiatives that will influence the process. Members and staff must discuss internal and external factors that could affect budgets over the next several years, including your organization's strategic plan. After approval, the committee monitors variances from the budget.

3. Financial reporting. The committee oversees the preparation and distribution of financial statements and sets expectations for the nonprofit's staff about the level of detail, frequency and deadlines of other financial reports. The committee monitors the adequacy of the organization's financial resources and the allocation toward accomplishing its mission. Simultaneously, the committee ensures that donor-restricted contributions are being met. Additionally, the committee decides whether resources are sufficient to support expected program and operating expenses.

4. Developing internal controls. Internal controls are essential for protecting your organization's assets. Have your finance committee work with staff to develop effective controls and policies and document them in a manual. It's also up to the committee to make sure that approved controls are followed and filing deadlines are met.

5. Administering financial resources. The finance committee establishes and confirms compliance with fiscal and related policies and procedures. Approved policies should reflect your organization's specific circumstances, such as size and life-cycle stage, rather than just general "best practices." The committee should take care, though, not to overstep. It must respect the line between the oversight of overall policies versus the actual implementation and execution of specific staff processes and procedures.

6. Overseeing audits. If your organization doesn't have a separate audit committee, the finance committee is also responsible for the audit. The committee must engage and regularly interact with the auditors, review the auditors' report and IRS Form 990, present the audited financial statements to the board, and propose changes to implement any auditor recommendations.

7. Creating an appropriate investment policy. Even if your organization doesn't have enough cash to support a separate investment portfolio, liquid funds need to be managed to maximize revenue. This means it falls to the finance committee to develop an appropriate investment policy and retain qualified investment advisors, when needed. A separate investment committee is advisable, though, for organizations with substantial investments, planned giving programs or endowments. And remember that fiduciary responsibility isn't limited to the committee's members. The entire board has the duty to safeguard your organization's net assets.

The payoff

When a nonprofit has a vital and engaged finance committee, it sends a strong signal to stakeholders — namely, that the organization is committed to responsible stewardship of its financial resources and long-term sustainability. When your finance committee takes an active and strategic role in oversight and planning, the payoff will likely be robust financial governance and higher satisfaction levels of committee members. ■

Charge it!

Credit card issues for nonprofits

Credit cards are a common part of doing day-to-day business for most nonprofits these days. Donors typically use credit cards to make contributions, whether one-offs or recurring, and employees often rely on the cards when procuring supplies and services or traveling on behalf of their organizations. Some nonprofits have, or have considered, so-called "affinity cards" as a way of increasing revenue. Here are some things to think about if your organization finds itself in any of these circumstances.

Taxability of credit card rewards

Credit card rewards — including points, miles and gift cards — generally aren't considered taxable income by the IRS, especially if they come with a spending requirement. But some exceptions apply, and they could arise if your employees charge expenses for the organization.

For example, if an employee uses a personal card to pay a business expense, and you reimburse the staffer, a cash-back reward on the charge might be taxable income for the employee. If your employees have "corporate" cards and you allow them to keep related rewards for their personal use, the IRS considers the rewards to be taxable income to the employees. Your employees should check with their accountants in these situations, so they don't trip up at income tax time.

Deductibility of donated rewards

Credit card rewards can also come up in the context of contributions. You may have donors who wish to direct their miles or points to your organization. But they might expect tax benefits they won't actually receive.

As previously stated, the IRS generally doesn't treat such rewards as taxable income. The flip side is that the IRS also doesn't allow taxpayers to claim a charitable deduction for donating rewards. Your donors could, however, get a deduction if they redeem their rewards for cash and then donate the cash.

Treatment of recurring donations as subscriptions

In the fall of 2022, Mastercard implemented a new rule for recurring payments. Among other things, the rule requires businesses with such subscription arrangements to send Mastercard members an email or other electronic communication with opt-out information every time a payment is charged.

Mastercard initially indicated that it would treat recurring donations as subscriptions subject to the new requirements, with the rules beginning to apply to nonprofits on March 22, 2023. The company has since retreated on that stance. While the requirements remain recommended "best practices" for nonprofits, an organization will be required to comply only if its recurring donation program experiences an "excessive" number of chargebacks or consumer complaints for four consecutive months.

Credit card rewards — including points, miles and gift cards — generally aren't considered taxable income by the IRS.

Affinity card debate

Nonprofit affinity credit cards — charity-branded cards where the organization receives a percentage of a cardholder's purchases — have come under criticism in recent years. For starters, the contribution percentage often is quite small. Moreover, if improperly structured, these arrangements could result in unrelated business income tax for the nonprofit.

But the cards can have benefits beyond just the bottom-line contribution revenue. They can, for example, increase engagement with supporters. They also might provide a low-cost marketing benefit, creating awareness and opportunities for users to talk up the organization when they use their cards at checkout. And affinity cards give prospective supporters who don't want to have to think about it or who otherwise wouldn't donate an easy way to show support.

We can help

Have questions about the tax or operational implications of various credit card uses at your organization? Give us a call. ■

NEWSBYTES

IRS set to deactivate foundations' electronic payment accounts

The NonProfit Times recently reported that the IRS is shutting down the Electronic Federal Tax Payment System (EFTPS) accounts of certain private foundations. Private foundations with more than $500 in excise tax liability are required to use the EFTPS to make their tax payments. But for security purposes, the agency is deactivating accounts that haven't been used for 18 months. According to the *Times*, the IRS hasn't alerted any foundations at risk of having their accounts deactivated before doing so.

Private foundations should verify that their EFTPS accounts are active sooner rather than later. Deactivated accounts require re-enrollment as the prior accounts won't be re-opened — they've been purged from the system. On re-enrollment, organizations will be mailed personal identification numbers (PINs). Those that wait until their payment deadlines to re-enroll may find they don't receive their PINs in time to submit their payments via EFTPS by the applicable due date. ■

How Microsoft is expanding support for nonprofits

Microsoft is expanding its nonprofit technology offerings to public libraries and public museums. Eligible organizations can obtain discounts for cloud solutions like Microsoft 365 and Office 365 (including Teams, Outlook, Excel and PowerPoint), Azure (for project management), Dynamics 365 (for relationship management), Power Apps (for building and sharing apps) and Surface devices. They'll have access to on-premises licenses for computer labs and other public access devices, too.

Libraries and museums will also be eligible for grants that cover the cost of Microsoft 365, Azure and Dynamics. In addition, Microsoft Advertising is offering a $3,000 monthly grant to help all nonprofits reach new visitors, donors and volunteers. The grants apply to the company's owned-and-operated digital search and native advertising platforms such as Bing. ■

Donation option at checkout stresses retail purchasers

A study published in the *Journal of Business Research* calls into question the common belief that consumers feel good about making charitable donations as they pay at stores or restaurants. The study finds that many people experience negative feelings in these situations — including feeling "pressured," "annoyed" and "concerned about being judged." Only about 20% of the words participants in the study chose to describe their feelings about so-called "checkout charity" were positive, such as "nice" or "compassionate."

The researchers found that checkout solicitations induce customer anxiety, in part due to the pressure to make a hasty decision. Although the anxiety can drop in "solicitation episodes" where customers agree to donate, this occurs only when the request is made by an employee, as opposed to requests from self-checkout technologies like kiosks. While the study was intended to caution retailers, nonprofits also should consider the potential negative consequences of checkout solicitations. ■

LAPORTE
CPAs & BUSINESS ADVISORS

111 Veterans Memorial Blvd, Suite 600 | Metairie, LA 70005-3057
504.835.5522 | FAX 504.835.5535

ANNUAL NONPROFIT EDUCATIONAL SERIES

LaPorte CPAs & Business Advisors has a proud history of serving the nonprofit community. A principal component of that commitment is sharing our knowledge and resources with nonprofits in the communities we serve.

In its ninth year, our annual Nonprofit Educational Series was developed to provide information on a wide variety of topics that affect the nonprofit community. These events were presented by LaPorte nonprofit industry leaders and recent topics have included building an effective board, nonprofit ethics and the Form 990, and changes in tax laws, to name a few. A few sample recordings of these presentations can be accessed at **https://bit.ly/LaPorteNonprofitSeries**.

We are in the early planning stages for our next Nonprofit Educational Series, currently slated for Summer 2023. Because this series is meant to provide information on topics of interest to you, please let us know if there are particular topics that you would like us to cover by emailing Nonprofit Industry Group Co-Leaders Dawn Laborie, CPA, at dlaborie@laporte.com or Jack Wiles, CPA, at jwiles@laporte.com. And be on the lookout for invitations to follow later this Spring!