FrankelZacharia LLC

Certified Public Accountants

Nonprofit Cybersecurity: Why it Should be a Top Business Priority

With cyberattacks on the rise, even nonprofits can no longer ignore or poorly budget for this serious problem. Groups that may want to disrupt your mission or hold your data hostage may use malicious action to break into your system and use the data they obtain for nefarious purposes. As an example, a recent attack revealed the confidential details of over a half million people being served by the International Committee of the Red Cross. No motive was stated, and the responsible party still hasn't been held accountable, but people's critical data was put at risk.

From donor payment information to individuals receiving services, the fact that your organization undertakes noble causes doesn't detract from its appeal to cybercriminals. Good intentions won't mitigate short- or long-term impacts of a cyberattack. This means that your nonprofit's cybersecurity must be a top priority for your organization, regardless of current IT infrastructure, budget or mission.

How Is Nonprofit Cybersecurity Different?

Nonprofits often face unique challenges over the years. Though many cyber concerns overlap with those of private companies, their public work creates additional vulnerabilities. These issues can include:

- **Inside jobs.** Though these are usually accidental, with some actually being malicious, they both deliver the same outcome, with private data being put at risk. According to more recent research, insider threats have increased 44% over the past couple of years.
- **Cause-driven attacks.** If organizations support a polarizing cause, those who are against that cause may try to maliciously attack the organization to disrupt its operation and purposely cause harm to its mission.
- **More complex.** Because cloud and mobile technologies have been adopted so readily the past two years due to the COVID-19 pandemic, data is at risk from these new communications options. The risk also adds to complexity, as companies must determine who is accessing what data at what times for which purposes. This allows attackers to compromise systems without detection.
- **Public data sources.** Because nonprofits have a higher level of data transparency than other organizations, they're at a higher risk to attack while being subjected to greater scrutiny. This can create serious problems for cybersecurity.

How Nonprofits Can Boost Cybersecurity

To improve informational security for your nonprofit organization, you'll want to start by taking a multifaceted approach. Though individual technologies and tools can pinpoint particular attack vectors or mitigate any damage that occurs, it won't defend your organization from ongoing, evolving attacks. At that point, hackers may go after user accounts to gain access to your systems, move laterally through programs or simply wait and collect data until they're ready to strike. Here's a quick look at three industry best practices that can help your nonprofit organization stay secure:

- **Keep cybersecurity at the forefront of all plans and practices.** You can't add it as an afterthought. Instead, information security expertise needs to be at the planning table in the C-suite. By making it a vital part of the decision process, you can minimize your total risk.
- **Recognize the differences between due diligence and due care.** Because nonprofit organizations must demonstrate both, it's important to understand the differences. “Due care” refers to guidance and direction when creating a cybersecurity framework while “due diligence” refers to the act of following the guidance and policies.
- **Make sure policies are consistent.** Your cybersecurity policies must apply to everyone in your organization, from front-line staff to C-level executives handling long-term strategy. If you don't have consistency, the policies won't have as strong of an impact as you would want.

Steps You Can Take to Reduce Your Risk

Keeping up-to-date reduces your nonprofit's risk. There are a wide range of resources from the U.S. Department of Homeland Security that can help you understand your threat landscape and how it impacts your operations. After gathering resources, conduct an audit using a trusted third-party company so that you can pinpoint cybersecurity problems that may not be obvious. Consider your eCommerce storefront if you have one. Often used to drive donations while improving social awareness, having this data hacked puts your donors' personal and financial data at risk. Take care to stay in compliance and make sure that data is protected.
Nonprofits also need to build a comprehensive security program that has been designed to address all the facets in your risk landscape. By taking this type of approach to your organization's cybersecurity needs, you can identify and fix the basic causes of your common security problems instead of simply trying to work on the symptoms, giving you a stronger overall security standing.

In Conclusion

By strengthening your overall cybersecurity position, you'll be able to better protect your organization and its mission against the possible risks cybercriminals bring to the table.

If you have any questions or would like additional information, please contact Frankel Zacharia at (402)496-9100 or www.fzacpa.com