Building Support from Staff and Donors for your Nonprofit's Cybersecurity

October is National Cybersecurity Awareness Month. We've been proud to partner with the National Cybersecurity Alliance and the federal Cybersecurity & Infrastructure Security Agency for several years in efforts to bring resources to nonprofits. While I was tempted to write another article with some tips and tools, I want to go in a different direction this year. (If you are still interested in those tips and tools, I recommend checking out this year's #SecureOurWorld campaign site.)

Instead, I want to focus on something more elemental: building support for cybersecurity, both internally with your staff and externally with donors and funders. Without that support, those tips and tools will be a lot less effective.

Building internal support

The strength of your organization's cybersecurity isn't about how many IT staff you can afford or how much you spend on a particular system.

> Your nonprofit's cybersecurity is only as strong as the weakest link on your staff.

It only takes one person to open a link in a phishing email to render the most sophisticated system helpless. It takes just one person sending a password by email, instead of using the organization's password manager. Cybersecurity can't be successful if it's the job of just your IT person; it must be the job of every person at your organization.

There are many elements to the culture of a nonprofit. Make sure cybersecurity is one of them. The person in charge of IT matters can start with conversations with your executive director and other senior staff. Help them understand the importance of reminders about cybersecurity best practices. Get their buy-in on regular phishing tests and cybersecurity training for the whole staff. If they can lead by example in taking the work seriously, it helps with buy-in across the rest of the team. (By the way, conducting phishing tests and providing cybersecurity training can be relatively easy and inexpensive. Groups like TechImpact can help you get started. And you may find that, when people know they're being randomly tested, they become more vigilant about watching for cybersecurity threats and complying with established defensive protocols.)

Building external support

Ok, so you've secured the support of your executive director and spread the word internally. But now how do you get the resources to take the next step? For too long, nonprofits have been afraid to spend money on cybersecurity. A lot of that hesitation has its roots in the old "overhead myth," where donors were told to evaluate nonprofits based on the overly simplistic ratio of how much they are spending on program versus overhead.

There is no need to be defensive about investing in vital infrastructure for your organization to be able to deliver those programs. More than anything else, donors and funders appreciate transparency from the nonprofits they support.

> Be proactive and transparent about how their contributions are being used to keep information about them and about the people you serve secure.

Now, I’m not saying that a capital campaign to implement a new donor management system is going to be a wild success. But you can be telling your current and potential donors how important your nonprofit finds safeguarding their information. You can talk in grant proposals and reports, not just about the people your nonprofit helps, but also about how you are protecting sensitive case information about those people and personal information about your employees, board members, and donors. You may be surprised by the positive responses you receive.

Once you have that internal and external buy-in, the work of protecting your nonprofit’s systems and information will be much easier – and those tips and tools will be much more effective.

Resources

- Secure Our World (Cybersecurity & Infrastructure Security Agency, part of the US Department of Homeland Security)
- How To Build a Culture of Security at Your Nonprofit (Dan Rivas, TechImpact)
- Keeping Your Nonprofit’s Website and Data Secure (Rick Cohen, National Council of Nonprofits)
- Cybersecurity for Nonprofits (National Council of Nonprofits)