Feeling Insecure About Security? Protecting Your Nonprofit's Data Is Not Rocket Science

By: Adam White

If you, like many other small nonprofit leaders, are finding yourself increasingly worried about the security of your organization's data and are looking for a quick and easy solution, I have some bad news: there is no quick fix to putting your nonprofit's worst cyber-attack nightmares to rest. The good news is that addressing this issue does not have to create a budgetary nightmare.

The fine folks at Idealware, a leading nonprofit that provides technology guidance to other nonprofits, recently released a report detailing practical steps nonprofits can take to protect their most important data. Best of all, you don't need to be an IT professional to make sense of it.

The report issues an important wake-up call, insisting that no nonprofit or business is too small for hackers to notice. The fact is, small nonprofits often make perfect targets precisely because they are not protected by security teams like many large companies are. Additionally, if your nonprofit has any type of online presence, it can be penetrated using software that scavenges the internet and sends out automated attacks without requiring the hackers to have any prior knowledge of the targets.

The donors, volunteers, employees, and any other stakeholders whose personal information your nonprofit stores are trusting that their data will be kept safe. And depending on what type of information your organization collects, it may be required to meet specific security regulations.

Worried yet? Before you get overwhelmed or begin to clear room in your organization's budget, consider these practical and inexpensive security tips offered in Idealware's report that I am confident any nonprofit can handle:

Physical security

The majority of security breaches are caused by natural disasters or by improper employee activity. The way your nonprofit's office is configured can go a long way toward protecting its data from these types of breaches. Keeping doors locked and locking up sensitive information, such as employee or donor records, is a good place to start. However it is likely that your nonprofit stores many of these sensitive records digitally. Any devices that contain organization data (laptops, computers, printers, etc.) should be locked in a way that prevents the device from easily being carried away from the office (i.e. secured to a desk or locked in a cabinet when not in use). Aside from the old lock and key strategy, it is critical to ensure all computers are logged off at the end of the day. Installing automatic screen locks is an easy way to take care of this.

In order to guarantee your nonprofit is able to retrieve its data in the event of a breach, it is imperative to back up its data offsite. After all, keeping an external hard drive in the office is not likely to protect your nonprofit in the event of a fire or natural disaster. The current trend is to forget the external hard drive altogether in favor of reasonably priced automated Cloud backups. Though many skeptics are hesitant about trusting a Cloud vendor with their precious data, Idealware argues that *"most nonprofits could not afford to maintain a fraction of the security that comes standard with a Cloud vendor."*

Online security

This is the area that strikes the greatest fear in most of us. If you're like me and the mere mention of terms like "firewall," "encryption," "SSID," or "WPA-2" is enough to give you a headache, it can seem a bit daunting to address. But unless your

nonprofit has no use for the internet, it is probably best to take an aspirin and familiarize yourself with basic online security measures. The following measures outlined in the Idealware report are simple but effective first steps.

- Automate software updates on all computers instead of relying on staff members who are prone to clicking the "remind me later" button.
- Install antivirus and antispyware software. Many of these programs are available for free or cheap, but you will need to do some research to decide which is best for your nonprofit.
- Check the wireless router and the settings on your nonprofit's computer operating systems to ensure that firewall protection is enabled. Firewalls (software that screens out viruses and hacking attempts) are often set by default in routers and operating systems, but it is prudent to double-check.
- Set a password for the wireless router that consists of many characters and uses several different character types. It is also wise *not* to publicly broadcast your nonprofit's Service Set Identifier (SSID), which is the name of the wireless network.
- Require every employee to have his or her own unique login name and password to access computers. This is a helpful measure because it makes it easier to trace the source of questionable activity on your nonprofit's network and prevent individual employees from accessing organization data after leaving the organization. These passwords should be regularly changed.

Idealware offers a variety of more advanced security measures, but the steps outlined above offer a solid groundwork from protecting your organization from a security breach. It is important to keep in mind, however, that there is no way to protect against all possible attacks. The best your nonprofit can do can do is reduce its risk. Therefore, it is critical that your nonprofit has concrete policies and procedures in place both for preventing a data breach and for responding appropriately in the event of one. The importance of such policies is best summarized by James Snow of the Prospect Park Alliance in Brooklyn, who is quoted in the Idealware report saying: *"You're never going to have enough money to keep the bad people out. Being safe comes down to policies."*

If you and your organization are serious about cracking down on data security, I highly advise reading the entire report and making use of the wealth of resources Idealware has to offer. But at a minimum, remember Mr. Snow's words as the overarching theme to security. People, not technology, are the best defense against

a security breach. The more aware and educated your staff is about your nonprofit's security, the more secure it will be. And while written policies are important, it is even better to foster regular conversation with staff (perhaps during weekly meetings) to discuss reminders, concerns, and ideas regarding security.

You may not be able to protect against every possible threat to your nonprofit's data, but an estimated 90% of data breaches are preventable. And preventing them is not rocket science; it's policies, procedures, and people!

Resources

- *What Nonprofits Need to Know About Security: A Practical Guide to Managing Risk*
- *Payment Card Industry (PCI) compliance information*
- *Health Insurance Portability and Accountability Act (HIPAA) Standards*
- *Digital Impact Guide to Creating Data Security Policies*
- *Cloud Computing for Nonprofits* *by Patrick Callihan*