How To Build a Culture of Security at Your Nonprofit

By: Dan Rivas

No organization can ever be 100 percent secure, but nonprofits that create a strong security culture—one that actively promotes security awareness and a shared sense of mission around security—are much more likely to avoid many of the most common threats.

At your nonprofit, you can create and support a culture that values security and vigilantly protects the organization's systems and data.

Involve Staff in Writing Policies

Staff members want to keep your organization safe. Often, they simply don't know what is acceptable and what isn't. Clear policies and procedures are an important step toward building awareness and strengthening habits.

There are many ways you can involve staff members in the policy-writing process. You can facilitate a conversation at a staff meeting, interview people who are the primary users of particular tools, or lead policy review sessions that help you gather input from a diverse group of staff members.

By including staff, not only will you learn more about your systems and how to secure them, but also staff members will learn a lot about how and why particular practices help your organization reduce risk. And just as importantly, through participating in the process, more staff members will feel a sense of ownership in the policies they helped create and will feel a stronger sense of responsibility to protect and therefore abide by those policies.

Provide Cybersecurity Training

Did you know that the majority of nonprofits—almost 60 percent, according to NTEN's "State of Nonprofit Security"—do not provide cybersecurity training on a regular basis? Staff members generally want to do the right thing, yet often don't realize they're taking risks. Many of the most common security threats exploit a basic lack of awareness.

That's why it's important to educate staff members about the potential threats and your organization's policies for reducing and managing those threats. All staff members should receive cybersecurity training, both when they're first hired and in refresher courses about once each year.

IT Staff Need Ongoing Training

Technology changes quickly. So do the threats. Threat actors continue to search for vulnerabilities and new opportunities to do damage or make money. Once they find a way in, they typically are aggressive about exploiting the opportunity.

Invest in the careers of your IT staff members and protect against emerging threats by providing certification courses through organizations such as the SANS Institute, the InfoSec Institute, Cybrary, or the MIS Training Institute.

Integrate Security into Daily Life

Regular staff meetings are a great time to discuss security concepts. You don't have to talk security every meeting, but if you build in a monthly refresher, you'll keep the concepts fresh and create opportunities for staff members to ask questions or offer input.

Some organizations go further and take a campaign approach, scheduling specific communications about security, such as offering helpful hints or discussing recent news stories about data breaches.

If you use a communication platform such as Slack, you can create a space where staff members can participate in a conversation. And, of course, if you offer incentives, such as prizes for answering a question correctly or attending a meeting, you're more likely to get staff members to pay attention.

Test Your Staff

How do you know if the training and ongoing communications are sinking in? The most straightforward way is to create a simple multiple-choice test that staff members are required to complete. Some nonprofits go even further and create fake threats to test how alert staff members are to potential threats. A few security education tools make it easy to set up fake phishing emails that give the recipient feedback based on what actions they take.

For example, if they delete the email, they might get a "Congratulations" message, but if they click a link, they can be directed to a webpage that explains how to detect phishing messages and what to do when a message looks suspicious.

Test Your IT Response

If a data breach occurs, will you be ready? One way to find out is to run a drill. Create a scenario, such as a ransomware attack, and then watch your IT staff go through the steps of cleaning up the machines and reloading data. Periodically test other scenarios, such as fire damage, a data breach, or malicious activity by a staff member so you can be confident that your team is prepared to respond quickly and effectively during an incident.

Show That You Value Security

One way to send a strong signal that you value staff members who take security seriously is to include cybersecurity in performance reviews. If you send out quizzes, use the scores as a starting point for a conversation. If a staff member hasn't been participating in training or has a history of poor security practices, you might factor

that into their performance evaluations, which could influence subsequent salary increases or promotions.

Keep the Conversation Going

Whichever methods you choose to involve staff in strengthening your organization's security, the most important element is signaling that you value their input and want to partner with them to achieve the shared goal of keeping your organization's data safe. By listening to the staff members who use your organization's technology every day you'll learn a lot about how people work at your nonprofit and they'll feel just as invested in the organization's security as you do.

Want to learn more about how to improve security at your nonprofit? Our free publication, *What Nonprofits Need to Know About Security: A Practical Guide to Managing Risk,* shows you how to assess your risk and what the basic protections are and provides a one-page security checklist that you can print and distribute to your entire staff. Get it at https://bit.ly/2X15bXy. You can also learn the basics of how cyberattacks happen and how to prevent them, and receive practical tips for how to respond in the unfortunate event of a breach by signing up for ***Cybersecurity Essentials for Nonprofits***, which runs Thursdays from September 23 through October 7 and costs $150. Learn more or sign up at https://bit.ly/3zXOwmh.

Dan Rivas is a contract writer for Tech Impact, a 501(c)3 nonprofit that provides technology education and solutions for nonprofits. Browse its Technology Learning Center for hundreds of free publications and downloads, a free organizational tech assessment, and a comprehensive curriculum of webinars, courses, and on-demand learning about technology created expressly for nonprofits at https://techimpact.org/technology-learningcenter.