Making Net Gains

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity

Staying Safe While Making a Name for Your Nonprofit on the Internet

The following article is adapted from a chapter on managing the risks of Web functionality and content featured in a new book by the Nonprofit Risk Management Center titled: Full Speed Ahead: Managing Technology Risk in the Nonprofit World.

Given how easy it is to establish that increasingly important billboard on the information superhighway, it would appear that the attendant risks couldn't be all that difficult to manage. If only that were so. The ease with which an entry-level employee can post a reasonably interesting website bears no relation to the risk you encounter when you get off the side streets and pull into the fast lane on the aforementioned superhighway. But with equal doses of caution, common sense and curiosity, every nonprofit can start to get a handle on the risks associated with a Web presence.

Web Functionality and Security

Whether you've got an in-house webmaster or rely on an outside consultant to post information to your site, it's unlikely there are more than a handful of people (if you're lucky) in your nonprofit who truly understand how — from a technical standpoint — the website works. This could be troubling if you encounter a problem with your website and prompt action is required. For example:

- A donor casually perusing your website discovers some profane content. He or she contacts headquarters (or worse, a board member) to withdraw a large pledge and express his disgust with the organization.
- A popular columnist, through her attorney, sends a cease-and-desist letter to your board chair demanding that you remove "stolen" content from your website.
- You discover that a former employee has created a website that parodies your nonprofit. Based on the calls you have been receiving about it, the site appears to be generating a lot of traffic.
- At a weekly staff meeting your customer service representative reports that product sales have gone from record-breaking high to record low levels over the past few days. In fact, no sales have come through the website since Tuesday. When you type in your nonprofit's URL in your Web browser, you discover that your shopping cart system, or worse, your entire website is "down."

The expression, "stuff happens" is true with respect to almost every project a nonprofit undertakes, including its use of technology and connection to the Internet. Unlike other categories of "stuff," however, technology-based events have the potential to reach and affect huge numbers of people and cause damage that can rapidly eclipse the ability of a nonprofit's financial or human resources to respond. So an extra dose of caution is required in managing these risks.

We invite you to consider using or adapting the measures described in the next section as part of an overall strategy for managing the technology risks facing your nonprofit.

Risk Management Strategies for Web Functionality and Security

Step 1. Raise Awareness

- As part of a larger process to engage your paid and volunteer staff in the nonprofit's commitment to safeguarding its vital assets (people, property, income and goodwill) and ensuring the safety of clients and other personnel, raise awareness about technology risks among these key stakeholders.
- Empower key personnel to take responsibility for safeguarding technological resources. All staff should be encouraged to report anything unusual with respect to the website; raise any concerns they have about the safety of equipment, software, data and records; or suggest additional strategies for protecting technology resources.

Glossary of Technology Terms

These terms are among those featured in the full glossary for Full Speed Ahead: Managing Technology Risks in the Nonprofit World.

Meta tag — Words contained in code — not visible on a website — but detectable by search engines. Incorporating trademarks as meta tags may constitute trademark infringement.

Reverse domain name hijacking — The owner of a trademark causes the first user of a domain name (which happens to be similar or identical to the trademark) to lose its domain name. See Giacalone v. Network Solutions, Inc., 1996 WL 887734 (N.D. Cal. 1996) (TY.COM versus Ty, Inc., the maker of Beanie Babies).

URL – Uniform Resource Locator — A string of characters that represents the location or address of a resource on the Internet and how that resource should be accessed. World Wide Web pages are assigned a unique URL. The address of a website is usually in a format such as http://www.siteaddress.org.

Web browser — Also known as a Web client program, this software allows you to access and view HTML documents. Netscape Navigator, MSIE, Mosaic, Lynx, WinWeb and MacWeb are some examples of Web browsers.

Web walking — Using a Web client program to move through the documents available on the World Wide Web. This casual browsing nature of navigating the WWW has also been referred to as strolling, crawling and jumping.

Webmaster — A person or group of people who maintain and administer a Web server. Webmaster also refers to a standard e-mail address at most Web hosts where comments and questions can be sent.

Step 2. Make the Assignment

- Consider assigning responsibility for routinely perusing your website to verify that it's functioning in the way intended. The MIS Director or other lead "techie" on your staff should be alert to the possibility and consequences of Web malfunctions.
- Make sure you have a back-up staff person for technical issues, including the operation of your website. Your technology nightmare could easily occur while your "techie" is camping in the Adirondacks.

Step 3. Evaluate Your Web Security

- If your website is hosted by an outside provider, what do you know about the company? Request information on the provider's security features and precautions. Find out what steps you should take if you suspect a breach in security. How secure is the information transmitted via your website? Less than five years ago, having a "secure server" for e-commerce functions on a website was prohibitively expensive and out of the reach of small and mid-sized nonprofits. Today a number of vendors provide services that enable a moderately sophisticated user to set up a shopping cart system linked to a secure server hosted by an Internet Service Provider.

Step 4. Create and Test Your “Cut Off” Plan

- Make certain that more than one staff member at your nonprofit knows how to terminate the operation of your website in the event of an emergency, such as the discovery of a worm or profane, pornographic or otherwise offensive content. If you’re hosting your own website (your Web server is on the premises), you’ll need to have a written procedure so that a non-technical manager can shut down the site in the event of an emergency. If your website is hosted off-site by a vendor, you’ll need to contact your customer support representative to shut down the site immediately.
- Consider conducting a “drill” to test the above procedure. How long did it take to get the site back up and running? Run the drill with the MIS Director on site and try it without the MIS Director. Do you have a backup “techie”? Do you have written instructions kept off-site?

Step 5. Monitor and Manage With Care

- Always test new procedures on your website, preferably from within and outside the organization, before going live.
- To verify that your site is “up and running,” consider leaving your homepage up on one computer during business hours and clicking the “refresh” button from time to time, or setting your Web browser to automatically display your website when it’s launched.
- Maintain redundancy for your website, and test all new pages on a staging platform (a separate server or drive that is not publicly available and from which you can replicate your Web content to your public site) before going live on the Internet.
- Consider registering multiple domain names for your nonprofit. The usual suspects are your preferred domain name with .com, .net and .org extensions. The availability of a new list of extensions (such as .biz, .info and .pro) increases the difficulty of the selection process. After identifying the obvious candidates, consider asking one or more Web users who are not formally associated with your nonprofit to guess what your nonprofit’s domain name might be. Use the results of this informal survey to develop a list of candidates for registration. But don’t try to purchase every domain name pertinent to your nonprofit — to do so would consume considerable financial resources, not to mention creativity better spent on other activities. After registering various domain names, have these new URLs point to your official website.