

# Manage Increasing Internet Liabilities

BY JEANNE DEBUS

There is no question that the Internet plays an important role in a nonprofit organization's marketing and development activities. Nonprofits use their websites to educate the public about their mission, solicit contributions and attract volunteers and corporate sponsors. Many nonprofits have become very sophisticated with their websites, incorporating streaming video, RSS feeds, blogs, online giving and charity-based e-commerce portals. Social networking has become popular as well, with nonprofits relying on Twitter, Facebook, MySpace, etc., to help spread the word about their organizations and build brand awareness.

Many of these Internet activities stem from the proliferation of advanced technologies to facilitate a more seamless, secure and robust online experience. In the case of online giving, that trend has been driven to a large extent by the younger generation's greater affinity for performing many routine tasks online, including donating to their favorite charity. Additionally, it is believed that some of the high-profile disasters experienced over the past several years also have fostered a greater reliance on the Internet. Following 9/11 and Hurricane Katrina, for example, there was a significant increase in online giving that subsequently gave it greater recognition as a cost-effective way to generate funds quickly in a crisis situation.

At the same time, there are risks associated with the Internet, which nonprofits must recognize and manage effectively.

## Beware of Common Cyber Liabilities

Activities across the World Wide Web are governed by various laws. They range from privacy legislation (e.g., the Health Insurance Portability and Accountability Act and the Fair Credit Reporting Act and Privacy Act of 1974), which regulate the use and protection of personal information, and spam legislation (i.e., CAN-SPAM Act of 2003) which mandates the identification of unsolicited commercial emails and requires senders to give recipients the option to opt-out of their emails, to communications decency laws (e.g., Communications Decency Act), which regulate user-generated content and require compliance by Internet Service Providers and bloggers.

Another law that regulates certain activities on the Internet is The U.S. Copyright Act. It is designed to protect others' intellectual property and prohibits the misuse of others' trademarks and/or the use of others' copyrighted material without their express permission. Very often, organizations will simply copy and paste onto their websites information they think would be valuable for their audience or supports their mission without first securing the copyright holders' permission. This is an infringement of the Copyright Act.

For nonprofits, a misstep such as this one by an employee or volunteer on its website, or relating to how an email fundraising campaign was performed, can result in a lawsuit involving heavy legal expenses and a potentially hefty fine.

In addition to legislation-related risks, nonprofits face potential technology-related liabilities. For example, a nonprofit's Information Technology (IT) system could fall victim to a hacker who proceeds to compromise the security of its donors' personal and financial information, as well as to compromise its own institutional records.

Whether associated with technology failures, privacy breaches or noncompliance with a law, these various liabilities pose first-party and third-party risks to nonprofits, such as the following.

### First-party risks:

- Privacy notification expenses
- Regulatory claims for failure to notify in compliance with various laws
- Cyber extortion and threat expenses
- Data recovery and business interruption expenses stemming from a failure to install the latest security patches, which results in a virus attack on the IT system
- Public relations and crisis management expenses

### Third-party risks:

- Privacy liability claims (financial and personal injury) brought by others due to a hacker breaching your own system or using your system to access and breach a third party's IT system
- Liability claims (financial injury) arising from the denial of service caused by a security breach of your own system or the use of your system to breach a third party's IT system
- An Internet advertising company's tracking the behavior of a donor on your website using "cookies," which privacy advocates consider deceptive and an invasion of privacy
- A vendor posting an ad on your website that includes slanderous information against another company (financial and personal injury)

## Effective Risk Management

While these risks do exist, they can be managed with proper education, precautions and insurance strategies. It is recommended that every nonprofit prepare an *Internet Liability and Risk Management Policy Handbook*. It should include a breakdown of various Internet-related risks and appropriate measures to prevent and/or minimize those risks. Among the risk mitigation measures that should be noted in the handbook and diligently followed are:

- The full enforcement of an information security policy to be followed by all employees, volunteers, contractors and other parties with access to your computer network/IT systems
- Ongoing monitoring of system security to ensure that optimum configuration, encryption, security patches, firewalls and up-to-date virus protection is in place and that the installation of any new devices do not compromise system security
- Automatic receipt of virus and cyber threat notifications from the U.S. Computer Emergency Readiness Team (US-CERT) or SANS Institute
- Remote network management using a Virtual Private Network (VPN) or comparable system



- Daily back-up of network data and configuration files, as well as the storage of back-up files in a remote secure location
- Maintaining locked server rooms and limiting access to authorized (i.e., need-to-know) personnel only
- Establishing an IT disaster recovery plan and security incident response plan that are tested for effectiveness and about which employees are thoroughly trained

An effective cyber-risk management strategy must encompass an Internet-specific liability policy. It should be carried in addition to the organization's general liability, professional liability, directors and officers, errors and omission and umbrella policies. There are many different Internet liability policies offered that vary from carrier to carrier. The coverage offered will be determined based on an initial assessment of the nonprofit's various cyber liabilities, its IT system security and related policies and the extent of its Internet activities (i.e., the complexity of the network;

how robust the website is; whether there are online giving, e-commerce and/or blog components; its email communications/fundraising practices; etc.). If a carrier deems that a nonprofit satisfies the minimum risk control standards, it will offer the right coverage with adequate limits.

Before purchasing a specific Internet liability coverage, nonprofits should read a sample policy and ask for clarification regarding the definitions and exclusions presented. As part of their Internet liability insurance strategy, nonprofits should require all of their vendors to sign a contract that includes a hold harmless or indemnification agreement in favor of the nonprofit. In addition, vendors should be required to show proof that their professional liability insurance also includes contractual liability coverage presented in the form of a certificate of insurance. As an added precaution, nonprofits should regularly check to make sure their vendors' insurance is maintained.

The Internet represents a wealth of

opportunities for nonprofits, but at the same time there are perils associated with its use. Courting online donors who, according to the *2008 DonorCentrics™ Internet Giving Benchmarking Analysis* by Target Analytics (a Blackbaud Company), give larger gifts than traditional donors, along with spreading the word about your mission. In addition, attracting volunteers and sponsors, etc., are all facilitated through the Internet. Using sound cyber-risk management practices, nonprofits can continue harnessing the power of the Internet for these purposes while avoiding unnecessary liabilities.

*Note:* The report *2008 DonorCentrics™ Internet Giving Benchmarking Analysis* can be downloaded free of charge at [www.blackbaud.com/files/resources/downloads/cam/TargetInternetGivingSummary2008.pdf](http://www.blackbaud.com/files/resources/downloads/cam/TargetInternetGivingSummary2008.pdf). ©

*Jeanne Debus is vice president at Cook, Hall & Hyde Inc., with offices in Melville and East Hampton, N.Y., and Fair Lawn, N.J., [www.chhins.com](http://www.chhins.com).*