Nonprofit Risk Management Center

…find the answer here

Handout Materials for Webinar
March 5, 2008

Managing Technology Risks: Employee and Volunteer Blogs, e-Commerce, and Internet Piracy

A Litany of Technology Risks – Do Any of These Worry You?

Screensavers with sexual content/graphics
Harassment via email, voice messages or instant messaging
Employees or volunteers driving while on their cell phones
The distraction of answering emails all day and multi-tasking
Employees or volunteers visiting web sites that contain pornographic material
Use of the nonprofit's computer for an employee's or volunteer's personal for-profit business
Employees using copyrighted photos or graphics without permission
Data loss through a crash, or a virus
Someone using spyware to steal financial or personal information from your web site
"Click fraud" invading your nonprofit's web site (pop-up ads that just keep multiplying when you click to close them)
Someone hijacking your nonprofit's web site and changing its look or content
Use of email by employees for solicitations/union organizing

> In an extremely management-friendly decision handed down in December 2007, the National Labor Relations Board (NLRB) has held that employees have no statutory right to use an employer's email system for union-related communications.

An employee's personal blogs discusses work-related issues and names the nonprofit
A visitor to nonprofit's web site provides personal financial information that is intercepted by hackers

Check List for Securing Your Nonprofit's Data*

Passwords are the most basic defense against data loss

- A combination of letters and number
- At least 6 characters

* Other helpful checklists and sample policy language is available from the Center's publication, *Full Speed Ahead: Managing Technology Risk in the Nonprofit World*

- ♣ Not obvious such as "password" your name, birthday or the nonprofit's name
- ♣ Private – only shared with the office administrator or HR
- ♣ Changed regularly, every 60-90 days
- ♣ Never written down and taped to the computer terminal!

-] Back-up Servers: using an off-site vendor that is reputable can enhance your ability to store data
-] Virus Protection Software:
-] Installing Firewalls in all the nonprofit's computers, including laptops
-] Training/orienting all staff to computer security measures they must respect and follow
-] Maintain confidential information such as employee personnel files and client data, also donor data, on a hard drive not accessible to network users, and use passwords to protect sensitive files/folders
-] Private Networks: using an outside vendor for your Virtual Private Network can help secure your data from intruders
-] Be aware of laptop theft; require employees to secure or keep laptops with them at all times. (Theft from cars and hotel rooms is most common.)

Fundraising Over the Internet

Charitable registration is a state-by-state obligation. Many states take the position that if a nonprofit's web site contains solicitation language and is accessible to its residents, the nonprofit is soliciting in that state. Consequently, many nonprofits decide to file for charitable registration in multiple states. To make multiple state filing easier, there is a multi-state filer project that has produced a, "Unified Registration Statement" that can be used to register in many states that accept the form. Each state may have additional forms/requirements for registration. Many nonprofits hire their accounting firms to conduct charitable registration filings and there are a few law firms that specialize in state charitable registration filing services (fee based).

Multi-state Filer Project web site: http://www.multistatefiling.org/
Uniform Registration Statement (URS)
http://www.multistatefiling.org/c_statement.htm

e-Commerce Risks

Links from a for-profit entity's web site can make it appear that the nonprofit is advertising/selling a for-profit's goods on its own site (running the risk that the nonprofit could lose its tax-exempt status or be penalized for engaging in a private benefit transaction). A link to a for-profit entity's home page is not enough – if there is a product endorsement on the nonprofit's site, or a direct link to a page where a visitor can purchase a product, that could trigger liability.

Exclusive endorsements of products by the nonprofit or on the nonprofit's web site can create taxable income to the nonprofit if the for-profit entity that receives the exclusive endorsement has provided the charity with corporate sponsorship dollars. Corporate sponsorships on their own are generally not taxable income to the charity, however, the added wrinkle of

giving a for-profit the "exclusive" right to be a corporate sponsor is perceived by the IRS to be so valuable that the income the charity receives is equated to advertising income (as if the charity were advertising for the for-profit)

A nonprofit should not partner with a for-profit entity that sells products or services that are in conflict with the nonprofit's own values.

Taking personal and financial credit card information over the internet can result in identity theft if the nonprofit is not careful about protecting such information through the use of appropriate firewalls and credit card handling procedures.

What policies can address these risks?

- Product Endorsement Policy can state that the nonprofit will not endorse any commercial product at all; or only with authorization of the board of directors.
- Corporate Sponsorship Policy should clarify that the nonprofit will not accept sponsorships from corporations that do not exhibit values that are consistent with the nonprofit's mission; clarify that sponsorships by corporations are charitable contributions and not quid pro quo commercial transactions and that the board/appropriate person or committee of the nonprofit must approve all corporate sponsorships.

Protecting Reputation

Policies should address the need to protect the nonprofit's intellectual property, brand identity and good will in the community. Such policies include.

Code of Conduct

Photo Release - Photos should be used on web sites (and in print) only with permission of the subject. If the subject is a minor, then parents or guardians should sign the release.

Blog Policy - Employees who blog can damage the nonprofit's reputation – a Blog Policy can require approval prior to publication of any content that mentions the nonprofit; employees should not blog on the nonprofit's computers, during work time, unless the blog is sanctioned by the nonprofit.

Responsible Use of Technology - False e-mails can be circulated that appear to be from the nonprofit – If the perpetrator is a third-party, the nonprofit may only be able to conduct damage control, but volunteers and employees can be terminated or disciplined if there is a policy that applies to them.

Web Link Review -- Links from your nonprofit's web site to other sites can be misdirected or the links can become stale. Business practices should include a regular review of all links from your nonprofit's web site.

Protection of Name and Logo - Rigorously enforce any unauthorized use of your nonprofit's name and logo; periodically conduct a search of your nonprofit's name on the internet and see what comes up. Don't let others use logos that are similar to yours -- your reputation and branding as a service provider to the community can be damaged.

A malicious hacker can place unseemly content on your nonprofit's web site. Make sure more than one person knows how to "shut down" the web site (if your web server is on the premises) and that employees and

volunteers help guard the nonprofit's integrity and reputation by reporting anything unusual about the web site.

Instant messaging and Chat Rooms
Employees are distracted by constantly switching tasks and responding to emails. Add to those normal work-day distractions the added distraction of pop-up instant messages and invitations to join friends in chat rooms. Employers are permitted to monitor employees' use of instant messages and chat rooms. Employees should only spend time responding to instant messages and conversing in chat rooms for work-related reasons. Abuse occurs when employees believe that 'no one cares' or 'no one is looking over my shoulder.'

Policy Checklist (some basic sample policies are provided below)

- ⎦ Privacy Policy for Web Site
- ⎦ Terms of Use
- ⎦ Web site Disclaimer and Notice to Viewers of Proprietary Information
- ⎦ Web site links, web links disclaimer
- ⎦ Confidentiality
- ⎦ Code of Conduct
- ⎦ Responsible Use of Technology Policy and Employee Acknowledgment form
- ⎦ Web site security policy (can be incorporated into
- ⎦ Internet Access Agreement (for clients who are youth and are using the nonprofit's computers during a program or activity sanctioned by the nonprofit)
- ⎦ COPPA (Children's Online Privacy Rights Act) Compliance Procedures
- ⎦ Product Endorsement Policy
- ⎦ Corporate Sponsorship Policy
- ⎦ No-solicitation policy

Sample Technology Policy

Office Technology: Appropriate Use and Privacy

The [Name of nonprofit's] information technology systems (networks, software, and computers) are tools that are provided to employees to enhance productivity and performance on the job. Although limited non-business use may be permitted when on personal time (e.g. during lunch hour or after work), employees understand that such non-business use should create no expectation of privacy to any data, information, or files that are created or stored on the [Name of nonprofit's] information systems. The executive director or other employees may have a need from time to time to access an employee's computer or files.
P
In addition, employees are expected to exercise good judgment in their use of email and the Internet and understand that access to these media is a privilege, not a right. Passwords are to be changed regularly and not shared with any person external to the organization without authorization.

Examples of Inappropriate Uses of Technology

Any use violating law or government regulation
Use promoting disrespect for an individual, discrimination, or constituting a personal attack, including ethnic jokes or slurs
Viewing, copying, or transmitting material with sexual content
Transmitting harassing or soliciting messages
Using copyrighted material without legal right
Use for personal financial gain, or in a manner creating a potential conflict of interest for the employee or the Center
Defamatory, inflammatory or derogatory statements about individuals, companies or their product.

The failure to use good judgment or to abide by the [Name of nonprofit's] policies may result in suspension of privileges or other disciplinary action.

I have read and agree to abide by the Office Technology policy described above.

_____ _____
Signature Date

Sample Web Site Disclaimer and Notice of Proprietary Information

All materials posted on this site are subject to copyrights owned by [Name of Nonprofit] or other individuals or entities. Any reproduction or republication of all or part of any document found on this site is expressly prohibited, unless authorized by [Name of Nonprofit] or the copyright owner of the material. All other rights reserved

The names, trademarks, service marks and logos of [Name of Nonprofit] appearing on this site may not be used in any advertising or publicity, or otherwise to indicate [Name of Nonprofit]'s endorsement or affiliation with any product or service, without [Name of Nonprofit]'s prior written permission.

Although the [Name of Nonprofit] web site includes links providing direct access to other internet sites, [Name of Nonprofit] takes no responsibility for the content or information contained on those other sites, and does not exert any editorial or other control over those sites.

[Name of Nonprofit] is providing information and services on the Internet as a benefit and service in furtherance of [Name of Nonprofit]'s mission and makes no representation about the suitability or accuracy of this information for any specific organization or circumstance.

Resources

Full Speed Ahead: Managing Technology Risk in the Nonprofit World, available from the Nonprofit Risk Management Center, http://nonprofitrisk.org/store/full-speed-ahead.shtml or email us: info@nonprofitrisk.org
TechSoup is a clearing house for donated technology as well as information for nonprofits on technology topics http://www.techsoup.org/
(Helpful articles in the "Learning Center")

National Institute of Standards and Technology Computer Security Resource Center
(News, information and trainings on internet security issues)
http://csrc.ncsl.nist.gov
Online Privacy Alliance - Guidelines for Privacy Policies
http://www.privacyalliance.org/resources/ppguidelines.shtml
Helpful article on computer security tips:
http://www.civicus.org/csw/DIGITAL_SECURITY-No33.htm