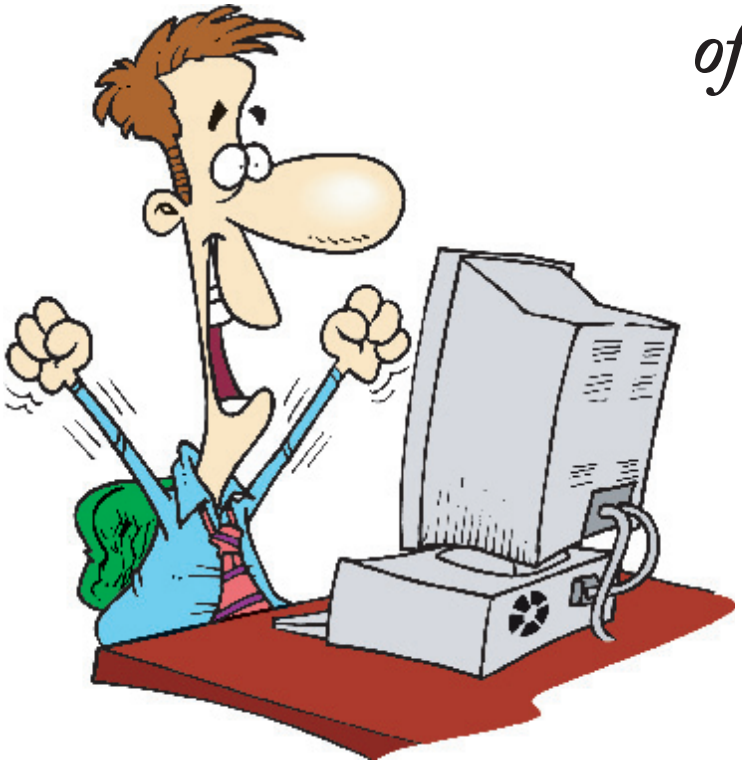
Managing

Technology Risks:

Staying on Course and Out of Trouble



Compliments of:

Nonprofits' Insurance Alliance of California

P.O. Box 8507 • Santa Cruz, CA 95061-8507

and

Alliance of Nonprofits for Insurance, *Risk Retention Group*

P.O. Box 8546 • Santa Cruz, CA 95061-8546

*www.*Insurance*for*Nonprofits.*org*

(831) 459-0980 or (800) 359-6422

Nonprofits' Insurance Alliance of California

A HEAD FOR INSURANCE . . . A HEART FOR NONPROFITS

Alliance of Nonprofits for Insurance

Risk Retention Group

About NIAC and ANI-RRG

Nonprofits' Insurance Alliance of California

Nonprofits' Insurance Alliance of California (NIAC) is a charitable risk pool governed by 501(c)(3) tax-exempt nonprofit organizations in California. NIAC is itself a 501(c)(3) tax-exempt nonprofit. At the writing of this booklet, NIAC insures more than 6,500 nonprofits in California.

Alliance of Nonprofits for Insurance, Risk Retention Group

Beginning operations in 2001, the Alliance of Nonprofits for Insurance, Risk Retention Group (ANI) is modeled after, and is an affiliated organization to, NIAC. ANI provides insurance to the charitable nonprofit community outside California. ANI is a 501(c)(3) tax-exempt nonprofit. At the writing of this booklet, ANI insures more than 2,000 nonprofits in 23 states and the District of Columbia.

Members of these two organizations purchase a variety of insurance coverages from NIAC and ANI including general liability, directors and officers liability, improper sexual conduct liability, commercial auto, and many others. Property and accident coverages are also available.

In addition to providing insurance coverages, both NIAC and ANI offer members a variety of free risk management and loss control services. These services include driver training, access to legal assistance, newsletters, and a video lending library, all provided free of charge to members.

A series of educational booklets published by NIAC and ANI are also available free to member-insureds. Text-only versions of these booklets may also be downloaded and printed off our website at *www*.Insurance*for*Nonprofits.*org*.

Titles include:

- Arrive…Safe and Sound: Tips to help with your nonprofit's vehicle safety program
- Sound Advice for Functions and Events: Tips to help your nonprofit stage safer special events
- Nonprofit Directors and Officers: Key facts about legal liability and insurance
- What Nonprofit Managers Need to Know About Lawsuits
- Supervision of Children and Teens Never Includes Sex
- Managing Volunteers: Balancing Risk and Reward
- Managing Technology Risks: Staying on course and out of trouble (available on-line only)
- Surviving a Crisis: Practical Strategies for Nonprofit Organizations

If you would like to learn more about how NIAC or ANI can help you, you may call (800) 359-6422 or check out our web site at *www*.Insurance*for*Nonprofits.*org*.

Nonprofits' Insurance Alliance of California
A HEAD FOR INSURANCE . . . A HEART FOR NONPROFITS

Alliance of Nonprofits for Insurance
Risk Retention Group

Table of Contents

Managing Technology Risks: *Staying on Course and Out of Trouble*

Please note: *This booklet is designed to provide general information to help nonprofit managers better understand issues relating to technology risks. It does not provide legal advice of any kind.*

This publication was authored by Melanie L. Herman, Executive Director of the Nonprofit Risk Management Center, and produced by Nonprofits' Insurance Alliance of California (NIAC) and Alliance of Nonprofits for Insurance, Risk Retention Group (ANI) for their member-insureds.

Nonprofits' Insurance Alliance of California (NIAC)

Alliance of Nonprofits for Insurance, Risk Retention Group (ANI)

P.O. Box 8507 • Santa Cruz, CA 95061-8507

(831) 459-0980 • (800) 359-6422

www.Insurance*for*Nonprofits.*org*

Introduction

In less than a decade, the average nonprofit has moved from depending on typewriters and "snail-mail" to fully embracing the use of a wide range of high tech devices, from network servers with impressive speed and massive storage capacity, to combination palm-held organizers and cellular telephones, to sophisticated donor management software and interactive websites with e-commerce functions.

Few, if any, futurists accurately predicted the extent to which technology tools would enable the unimagined efficiency we enjoy today. And even those who could have imagined such a future for the business community would likely have predicted a decade-long catch-up period for nonprofits.

The lure of new and emerging business technology can be intoxicating. And nonprofits with effective fundraising strategies can hardly resist the temptation to acquire technology that will boost the organization's productivity, allow it to reach greater numbers of clients in need, or simply make the organization a more sophisticated, appealing recipient of future funding. But along with the tremendous timesaving and content-enhancing benefits of technology, comes an array of risks. Given the nature of cutting-edge technology, many of these risks are of the type never before considered by a nonprofit's risk management advocates. While the risk of a child suffering an injury on a camping trip may be one easily envisioned by the managers in a nonprofit, the risk of destruction of the office file server or inadvertent release of confidential client information may be just as unimaginable today as wireless email was a decade ago.

Just as there appear to be no limits to how technology will be harnessed to change our daily lives, there is no ceiling on the range of risks facing an organization due to its use of and reliance on technology. And as new technologies are embraced by nonprofits, new risks will arise.

The information that follows is a starting point for a discussion we invite you to begin in your organization about the specific risks facing your nonprofit. It focuses on five categories of technology-related risk facing nonprofit organizations:

- Employee Use of Equipment and Systems
- Client Privacy
- System Security
- Proper Use of Software
- Safeguarding Your Website

Part 1: Employee Use of Equipment and Systems

Few would argue about the tremendous productivity-enhancing aspects of computer hardware, software and Internet access. In a matter of seconds, a short business letter can be transmitted electronically where previously the same task would have required time to write or type the letter, prepare a mailing label, stuff the letter in an envelope, affix postage, and drop the letter in a mailbox. When a single message needs to be transmitted to a large group of recipients, email's efficiency and cost-saving attributes shine. And if you need to find out if a message has been received, simply pre-set your email program to provide a confirmation that your addressee has retrieved your message.

But the availability of sophisticated equipment and tools brings some unusual and perhaps unexpected exposures for a nonprofit employer. For example:

- while an employee may be reluctant to use the nonprofit's letterhead to send a letter advocating a controversial position on a matter in the public spotlight, she may be more likely to quickly type and send an email conveying the same message;

- while a normally shy staff member might be reluctant to berate a customer or vendor, the same employee might feel quite comfortable dashing off an angry email message containing "choice" language;

- while a manager in your nonprofit might know that discussing sexual conquests at the water cooler is ill-advised, he might forward a list of racy one-liners to a former college roommate using your email system to do so;

- while your finance director may think that by hitting the "delete" key he has destroyed a potentially damaging memo concerning action taken against an employee, the same letter, with details on its original and altered form could be produced in litigation and serve as evidence of the proof that the organization violated a state or federal law.

The potential harm to a nonprofit stemming from employee misuse of technology is staggering. From civil and criminal penalties for software privacy, to liability to third parties for inappropriate violations of client privacy, a nonprofit places a great deal of trust in its employees when it provides equipment and an electronic connection to the outside world. The survival and viability of your nonprofit may depend on how and whether employees uphold that trust.

According to a poll conducted in December 2000 by *NonProfit Times*, more than one-third of nonprofits polled report employee abuse of email and the Internet. Half of the responding organizations reported having a written policy concerning email use, and an additional 7% reported that they will soon have such a policy in place.

Every nonprofit can and should take steps to both educate its workforce about their role and responsibility in protecting the organization's assets, as well as the specific expectations the organization has with respect to employee use of equipment and systems. Never assume that the prohibition of a certain activity or use would be assumed by employees. It's far better to provide explicit instructions about your expectations at the outset of the employment relationship, with reminders about acceptable use provided from time to time and as appropriate. As with any employment-related policies, their effectiveness is seriously compromised if the organization establishes but ignores the policies it adopts.

Goals for a Technology Use Policy

Every nonprofit should adopt a policy covering both the privacy aspects of technology use by employees as well as appropriate use issues. Some of the critical goals of your policy should include:

- dispelling employee expectations of privacy with respect to their use of equipment and systems owned by the nonprofit, as well as privacy with respect to equipment owned by the employee but brought to the office for business use; and

- establishing clear guidelines: what constitutes acceptable use of your equipment and systems, what constitutes prohibited activities, and what the consequences will be for violating the nonprofit's policies.

Technology Policy Elements

Review your current Technology Use policy against the following list, to determine if it should be updated to include additional instructions or prohibitions:

- Notify employees up front that their email may be monitored – this invalidates an employee's reasonable expectation of privacy. According to the American Management Association, 40% of major U.S. companies monitor employee email. This figure is up from 15% who did so in 1997.

- Tell employees what is and what is not appropriate use of email. Your list of inappropriate or prohibited email might include messages that are inflammatory, defamatory, impolite, or contain profanity or other offensive language. Consider including guidance in plain language, such as telling employees to only send emails that they wouldn't mind having read in a room full of people they know.

- Explain your nonprofit's policy concerning use of the organization's equipment for personal purposes. Many nonprofits limit personal use of email and the Internet to break times. Others prohibit personal use altogether. The latter policy may be impractical. If you allow employees to make and accept personal phone calls, you should consider whether it's appropriate to also allow staff to send and receive personal emails and use your Internet access for occasional personal reasons. Some organizations are using or adapting more flexible language, such as:

  "[Nonprofit's] email and telephone systems are primarily for business use, but limited and reasonable personal use is permitted."

- Using language such as this works best when it appears in tandem with details on specifically prohibited activities or uses. You don't want to wind up in a debate with an employee about what is "reasonable."

- Specifically prohibit activities that should never constitute permissible use of your equipment, such as using the nonprofit's technology to look for a job, knowingly open a virus, sending or forwarding chain letters, communication that represents personal view as those of the nonprofit (such as letters to the Editor), disseminating harassing or offensive materials, expressing political views, or soliciting or advertising matters unrelated to the business of the nonprofit.

- Explain that use of your equipment and systems is a privilege, not a right, and that privileges may be suspended at management's discretion for any employee who violates the nonprofit's policies or demonstrates poor judgment in the use of equipment or systems.

- Suggest a strategy for reporting inadvertent policy violations to management. For example, you might encourage employees to notify their manager immediately if they believe they may have sent, forwarded, or received an inappropriate message, or viewed an inappropriate website.

- Caution employees about your strict prohibitions on copying licensed software owned by the nonprofit or others and the illegality of such actions.

- Indicate whether employees are permitted to install software, programs or files they have purchased or downloaded or whether they must first obtain permission from the person responsible for technology and software in your nonprofit.

Note: A sample Technology Use Policy is provided in Appendix A.

Additional Risk Management Strategies Concerning Employee Use of Technology

Here's a list of suggested risk management strategies your nonprofit should consider as part of an overall effort to manage the risks of inappropriate use of technology by an employee:

- Monitor employee email, but limit eavesdropping to instances where you have a legitimate business reason to do so. For example, don't make it a practice to snoop in an employee's "in-box," but consider having the messages of an employee who will be out for two-weeks forwarded to another staff member for processing. Or you might consider reviewing recently sent and received messages if your nonprofit receives a complaint from a client or vendor about online or email etiquette.

- Consider installing blocking or filtering software that protects employees and the organization from unwanted or inappropriate messages. Email systems can be set to automatically reject messages containing certain attachments, such as virtual basic files, which are a leading conduit for viruses. Other filters can be set to reject messages containing profanity or other inappropriate language.

- Vest a member of management with responsibility for implementing your nonprofit's technology policy, coordinating investigations of misuse, and suggesting additional policies or procedures relative to employee use of equipment and systems. Your technology use policy may require more frequent review than other employment policies, due to the fast pace of changes in the type of systems used by your nonprofit or the way you use technology. In addition, as unexpected events occur, such as an inappropriate use that you may not have imagined, you'll want to update your policy to reflect this prohibited use.

- Provide an opportunity for employees to ask questions and request clarification about the nonprofit's technology policy and related policies. This opportunity could be provided as part of your new employee orientation, and repeated during regularly-scheduled all hands meetings.

Part 2: Client Privacy

Protecting client privacy is an important goal for many nonprofits. Whether the organization provides emergency shelter for victims of domestic abuse, matches mentees and mentors or places children in adoptive or foster families, every nonprofit should take reasonable measures to safeguard personal information about clients.

The availability of computer systems has resulted in tremendous improvements in case management. Client information previously maintained in worn file folders can be tracked in a database and readily retrieved by those with a "need to know."

There is a push and pull relationship between the need to protect client privacy and the desire to use state-of-the-art technology to enhance efficiency and program management. We must accept that there is a slight loss of efficiency that comes with the need to adequately protect client privacy. By the same token, no system can be completely secure from breaches of privacy and still be functional. Striking the appropriate balance for your organization requires a thorough review of your programmatic needs and technological capabilities.

Risk Management Strategies to Protect Client Privacy

- Articulate your nonprofit's policy concerning client privacy and instruct all staff on the policy. For example,

  "[Name of Nonprofit] is committed to protecting the dignity and privacy of all clients. Staff will keep client information in confidence, disclosing only with full permission to those who have a need-to-know, and not disclosing confidential information through insecure means, such as unencrypted email, fax, or cellular telephones."

- Obtain permission before using photographs or other information about clients for public relations or marketing purposes. Always use a photo release form before including photos of your clients in an annual report or on your web site. Exercise extreme caution when using photos of children for any purposes. For example, if a photo of a child appears on your web site, identifying information should not be provided, such as name of the school the child attends or child's name plus the name of the town in which he or she lives. This information could be used by a predator to track down the child to victimize him or her.

- If your nonprofit maintains detailed client files that contain highly personal information about your clients, restrict access to these files to only those individuals with a specific need to access them. In some organizations highly personal information should be kept separate from information that several persons in the nonprofit may need to view from time to time. For example, monthly progress reports concerning a mentor-mentee relationship may be accessible by several departments within the organization, while the results of the initial intake process may not.

- Keep your systems secure and let employees know that the need to maintain client privacy is the job of everyone. Change system passwords on a regular basis and keep regular audit trails of information accessed on your database. When telecommuting employees leave the organization, change the access phone numbers into your system to prevent unauthorized access.

Part 3: System Security

Our fears about what is risky are often disproportionate to the actual risks of an event materializing. As writer John Ross explained in his book, *The Polar Bear Strategy: Reflections on Risk in Modern Life* (1999, Perseus Books), many Americans who are fearful of dying in a plane crash (a highly unlikely event), fail to take basic safety precautions such as using a seatbelt, which can be life-saving in the far more likely event of a car accident.

This lesson applies to system security as well. While many nonprofit executives have unrealistic fears about attacks by hackers and the theft of intellectual assets, they take too few precautions to protect against the most common threat: theft of computers and peripherals or the unwitting destruction of data by insiders. An estimated 80% of all data losses or threats come from persons inside an organization, while only 20% result from the efforts of outsiders.

Hacking Risk

Hacking of various types is on the rise, according to the CSI/FB1 2001 Computer Crime and Security Survey. The Survey solicited feedback from 538 computer security professionals in corporations, government agencies, financial institutions, medical facilities and universities. Ninety-percent of respondent reports incidents of Internet Access Abuse, up from 80% in 2000. In addition, 95% reported virus attacks, up from 85% the prior year. Forty percent reported system penetrations, up from 25% in 2000. Hacking is the unauthorized use of, or the attempt to bypass the security mechanisms of, a computer system or network.

Internal Threats

Yet despite these dramatic increases in threats to an organization's systems from outsiders, the principal threat facing the security of a nonprofit's computer network is from insiders. Your network could be damaged, destroyed or rendered inaccessible as a result of:

- Intentional destruction by an angry employee;
- Unintentional destruction by an employee with inappropriate access privileges;
- The malfunctioning of non-computer equipment, such as an air conditioning unit;
- Theft of equipment, components or peripherals by an insider or intruder;
- Unintentional downloading of a virus;
- Accidents involving employee destruction of equipment (e.g., the engineer spills his coffee on the server).

Given these real risks and the potential that you could arrive one morning to discover major components of your computer system missing or malfunctioning, a risk management strategy for system security is a must in any technology-reliant nonprofit.

Risk Management Strategies for System Security

Consider the following action steps to increase the odds your organization could survive the risks described previously:

- Conduct a thorough inventory of your computer systems and equipment, identifying each piece of equipment by brand, model, serial number, location at your facility, and purchase date for all equipment, as well as memory, processor, hard drive, and devices (e.g., CD-ROM drive, zip drive, etc.) for your computers. Don't forget to include equipment that may be offsite, such as laptop computers provided to telecommuting employees. Include CPUs, monitors, printers, scanners, servers, uninterruptible power supply units, routers,

hubs, switches, copies of software and any other equipment of value. Maintain copies of your current inventory onsite as well as offsite at all times. If available, keep a copy in your locked, fireproof office safe.

- Conduct a thorough inventory of your software and software licenses, noting brand names, version numbers, purchase dates, and licensing information. Once again, keep the inventory onsite as well as offsite.

- Keep the room containing your most valuable computer equipment, such as your file server, locked especially when your office is closed. Also, make certain that the room where your server is located is cooled and humidified properly.

- Conduct a periodic (perhaps twice-yearly) check of all office CPUs to make certain that they contain the memory and other components assigned and installed. Also review hard drives to make certain that no impermissible software has been installed.

- Never leave laptop computers sitting on desks when your office is closed or otherwise unattended. Keep these valuable but easily stolen pieces of equipment under lock and key.

- Conduct daily or more frequent backups of the data on your server and at least weekly back-ups of individual hard drives. Store back-up tapes off site or in a fireproof safe.

- Conduct twice-yearly "fire drills" of your backup procedure to test your ability to restore data using the backup tapes.

- Train staff on the technology rules established by your nonprofit. Provide explicit direction about the prohibition on downloading viruses or worms, and provide the information they need to identify files containing viruses before it's too late.

- Restrict network access privileges prior to terminating any staff member. Don't allow a staff member who has just been fired to access your network except under close supervision.

- Have a full disaster recovery plan in place and tested. Keep copies of the plan onsite and offsite and make sure that the plan can be implemented by any staff member with significant knowledge of your organization (not just the staff "techie"). Your MIS staff member may be on vacation when disaster strikes.

Part 4: Proper Use of Software

- Using software without an appropriate license to do so—a practice called "software piracy"— is an increasingly common crime. According to a 1999 study conducted for the Business Software Alliance, a consortium of software makers headquartered in Washington, DC, piracy cost $3.2 billion in lost retail sales of business software applications. That number is likely to have risen in 2000 and 2001.

- No sector in the economy is exempt from the risk of software piracy. And unlike other forms of white-collar crime, such as stealing a nonprofit's financial assets, software theft may be unwitting or unintentional.

- When a nonprofit purchases software, whether it is a database package, desktop publishing software, or a spreadsheet program, a license to use the software is included in the purchase. The license is sometimes imprinted on the packaging that you promptly destroy in order to open your purchase. Sometimes it's featured on-screen as you're loading the program. Software licenses differ to a substantial degree. Some programs permit multiple users to use the program at the same time. In some cases you can install on both a desktop computer and a laptop. The most restrictive software licenses limit use to one computer at one time.

Although there are no studies to confirm or deny the prevalence of pirated software, nearly everyone has seen organizations which were using software which was copied or where employees were told not to call technical support because "we don't have that program officially." Although it may be common, it is still illegal.

Another common violation of software licensing is the practice of installing software restricted to one computer on a server. The penalties for violating a software license can be surprisingly stiff. Violators can face civil penalties of as much as $150,000 per infringement for software piracy. Criminal penalties under Title 17 can be as high as $250,000 per offense and up to 5 years in prison, although these penalties are rarely imposed when software has been pirated in a business setting for business use. These penalties are most likely to apply when software is pirated for profit.

There are other, perhaps more likely risks—in addition to fines and prison time—that accompany using pirated software. For example, the use of pirated software has been shown to increase the risk of a virus infiltrating a computer network, and increase the risk of insurmountable technical difficulties, as the nonprofit user forgoes access to technical support and software updates and upgrades.

Big Brother, Big Business

There are two industry "watchdog" organizations dedicated to eradicating software piracy. The Business Software Alliance, based in DC, receives tips—both anonymous and with full details—about software piracy. The Alliance, a consortium of software makers, investigates allegations of software theft and misuse. The BSA Hotline is 1-888-NO-PIRACY.

The Software and Information Industry Association (SIIA), also based in Washington, DC, receives 25 – 50 calls per week. Most of these reports come from current and former employees. The Association conducts audits of organizations suspected of engaging in software piracy. An average of five to ten new investigations are launched each week. The process begins with a request to an employer to participate in a voluntary audit. Refusal to participate could lead to a suit filed by the Association on its members' behalf.

In one case involving the SIIA, a tip against a nine-member law firm based in Atlanta resulted in a finding that pirated software was being used. The law firm paid $108,679 to several software companies and promised to destroy unlicensed software, purchase replacement software, and strengthen software management practices.

Risk Management Strategies to Prevent Software Theft and Misuse

There are a number of strategies that can prevent software piracy that every nonprofit should con-

sider adapting as part of an overall risk management program. For example:

- Consider including a "software code of ethics" as part of your Technology Use Policy. The code might indicate that if an employee pirates software they risk being fired in addition to criminal charges and civil penalties. The code should specifically prohibit giving the nonprofit's software to outsiders as well as using software that wasn't purchased by the nonprofit on the organization's systems.

- Educate employees about the importance of only using legal, licensed and approved software. Your organization is far more vulnerable to viruses and resources are wasted by downloading pirated or "fun" software not needed for business purposes.

- A simple step that every nonprofit can undertake is to organize software licenses and software in three-ring binders contained in a central library maintained by your chief information technology staff person.

- From time to time, your MIS staff person should conduct a simple "software compliance audit" whereby he or she compares the number of licenses owned by the nonprofit with the number of copies of various software programs running on the nonprofit's computers.

- Also consider discussing the issue of software piracy at an all-hands staff meeting where the details of your Technology Use Policy are presented. Training tools such as videos and a Guide to Software Management are available at www.nopiracy.com or www.spa.org.

Part 5: Safeguarding Your Website

A nonprofit without a web presence is like a nonprofit CEO who doesn't face staffing and fundraising challenges: highly unusual. Some nonprofits even stake out a web address and offer a web site "under construction" months before they open a bank account and recruit the founding board of directors.

Given how easy it is to establish that increasingly important billboard on the information superhighway, it would stand to reason 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 web site 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. In the section below we offer a number of risk management tips organized around two major topic areas: web functionality and web content.

Web Functionality

Whether you've got an in-house web master or rely on an outside consultant to post information to your site, chances are there are only 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 web site and prompt action is required. For example:

- A donor is casually perusing your web site and 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 the nonprofit's web site.

- At a weekly staff meeting your customer service representative reports that product sales have gone from record-breaking to record low levels over the past few days. In fact, no sales have come through the web site since Tuesday. When you type in your nonprofit's URL in your web browser, you discover that your shopping cart or 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 readers to consider using or adapting the measures described below as part of an overall effort to manage the technology risks facing your nonprofit.

Risk Management Strategies to Protect Web Functionality

- As you engage all of your staff (paid and volunteer) in the nonprofit's commitment to safeguarding its vital assets (people, property, income and goodwill) and ensuring the safety of clients, encourage these key stakeholders to take responsibility for safeguarding technological resources, as well. 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, with the appropriate management personnel, or suggest additional strategies.

- Consider assigning responsibility for routinely perusing your website to verify that it is functioning in the way intended.

- Make certain that several staff in the organization know how to terminate the operation of your web site in the event of an emergency, such as the discovery of profane, pornographic or otherwise offensive content.

- Consider conducting a "drill" to test the above procedure.

- Always test new procedures on your web site before going live, preferably from within and outside the organization.

- To verify that your site is "up and running," consider leaving your homepage up on one computer during business hours, or setting your web browser to automatically display your website when it is launched.

- Maintain redundancy for your website and test all new pages on a staging platform before going live on the internet.

Web Content

If your nonprofit wants to compete for donors, volunteers, customers, staff members and attention over the web with several million charities occupying our planet, you'll need a website that does more than simply advertise your address and mission statement.

Many nonprofits already successfully:

- solicit donations on the web,
- recruit and screen volunteers, and
- sell products and services (from cause-related marketing of others' stuff to offering consulting services and charity-logo embossed casual-wear, nonprofits are selling and someone is buying).

The more investment you make in packing your website with informative content and useful links, the greater investment you will need to make in monitoring the site. The following section contains a list of suggested strategies for use or adaptation in a nonprofit as part of an overall strategy for managing technology risks.

Risk Management Strategies for Web Site Content

Consider centralizing responsibility for web site content review and approval within your nonprofit. In a very small, all volunteer group this task could be assigned to a board member or other responsible volunteer. In a mid-sized nonprofit the MIS Director might be the logical choice, while the Communications Director could be the appropriate designee in a large organization. Although you may rely on any number of content "contributors" for your website, it's worth the time and investment required having someone review all proposed content for posting. The reviewer might decide to use a checklist approach to ensure that the following issues have been verified:

- the content is consistent with or is in no way contrary to the mission of the nonprofit;
- the content contains nothing that might be considered obscene, offensive, or insensitive to a potential wide and diverse audience of web site visitors;
- verification has been obtained or there is a high degree of certainty that the nonprofit has a legal right to the proposed content, and that no material contained therein violates an owner's copyright in said material;
- if written by someone other than an employee, the nonprofit has obtained written permission to post the content on the website, and if conditions of the posting have been imposed by the owner/author, those conditions have been satisfied (e.g. that the content include a specific attribution to the original source);
- the content contains the appropriate references to the nonprofit and refers to the nonprofit as indicated by the organization's style guide or publishing rules;
- the content does not contain anything that could be construed as defamatory or disrespectful to any particular individual or organization;
- the site does not contain logos or trademarks of other organizations unless your nonprofit has obtained express permission to use these items;
- the links you're featuring on your website connect to appropriate websites.

A Word About Linking…

It's worth the time and effort to not only monitor the links you've set up on your website to ensure that they remain appropriate, but to also determine who's linking to your website. In doing so, one nonprofit discovered that it was described as a "partner" on another organization's web site, although no arrangement existed between the two organizations. There are now commercial services that can help you monitor links. For example, at www.linkpopularity.com you can track who's linking to your web site and set up your account so you receive a monthly email update.

Conclusion

Although a nonprofit organization can choose to avoid certain risks, perhaps by deciding not to sponsor outdoor events or by limiting unsupervised contact between vulnerable clients and adult volunteers, few if any nonprofits today can avoid altogether the risks associated with the use of computer technology. Technology has brought untold and immeasurable dividends to the nonprofit sector. By harnessing technology small, community-based organizations can have a national or even global reach. Yet the benefits and advantages of technology bring risk and responsibility. Protecting the security of your vital computer systems as well as the privacy of your clients are critical risk management tasks in the information age. With a little planning and equal measures of common sense and imagination, every nonprofit can ask the questions and take the precautionary steps necessary to manage technology risks effectively. And managing system-related risks need not consume a great deal of time or consume financial resources needed for mission-critical activities. The key to getting started is to identify areas and sources of vulnerability and begin taking manageable steps to prevent harm. Also necessary is giving some thought and attention to what your nonprofit will do and how it will cope should it face a serious disruption or complete loss of access to its computers. Having considered a wide range of possibilities and spending time implementing prevention measures and a recovery plan, your nonprofit will be in an excellent position to withstand computer disasters caused by insider error, natural disasters, or third-party theft.

For information on any of the topics addressed in this publication, or technology risks beyond the scope of this publication, contact the Nonprofit Risk Management Center at (202) 785-3891 or visit www.nonprofitrisk.org. The Nonprofit Risk Management Center is a nonprofit resource center located in Washington DC, serving nonprofits throughout the U.S.

Appendix A

SAMPLE

Office Technology Use and Privacy Policy

[Name of Nonprofit]'s information technology systems (networks, software, computers, and other electronic devices) are tools 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 [Name of Nonprofit]'s information systems. The Executive Director, Deputy Director, or other employees may have a need from time to time to access an employee's computer or files.

In addition, employees are expected to exercise good judgment in their use of e-mail and the Internet and understand that access to these media is a privilege, not a right.

Examples of Inappropriate Uses of Technology

- Any use violating law or government regulation
- Any unauthorized access to computer systems or networks
- Any use promoting disrespect for an individual, discrimination, or constituting a personal attack, including ethnic jokes or slurs
- Viewing, copying, or transmitting material with sexual or profane content
- Transmitting harassing or soliciting messages
- Transmitting unsolicited advertising
- Using copyrighted material without permission or legal right
- Any use for personal financial gain, related to a search for a job in another organization, or in a manner creating a potential conflict of interest for the employee or [Name of Nonprofit]
- Defamatory, inflammatory or derogatory statements about individuals, companies, or their product
- Any use that constitutes a waste of [Name of Nonprofit]'s resources, including network resources
- Sending or forwarding chain letters
- Any use of network or systems for recreational games or other recreational purposes
- Any use that involves corruption or destruction of data, including knowingly launching a virus, worm, or other malicious software.

The failure to use good judgment or to abide by [Name of Nonprofit]'s policies may result in suspension of privileges or other disciplinary action. If any employee discovers that he or she has unintentionally violated this policy, he or she should notify _____ immediately.

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

Employee signature: _____ Date: _____