Technology: Boon or Bust?

By Jennifer Chandler Hauge

Resource Type: Articles

Topic: Data Privacy, Tech Risk, Cybersecurity, HR Risk and Employment Practices

During a recent weekend I spent 24 precious hours with two close friends who live in distant cities—hours that made us feel giddy, as if we had stolen them from our otherwise work and family-filled days. In order to spend that time together we turned off our cell phones, ignored email and basically refused to be members of the perpetually wired world. It felt great. But that feeling is in strong contrast to the message below, sent from a staff leader at a cultural institution, who shared how awful it feels when you lose access to your nonprofit's vitally important technology resources:

"Earlier this week, our nonprofit's database server crashed and we now find ourselves in a near-catastrophic situation. This completely unforeseen event has left us blindsided. We are unable to access our most critical software, including financial/accounting, fundraising and collections management systems. And, more disastrously, we are unsure of the condition of the data housed on the server and whether we will ever be able to recover it. This data comprises nearly seven years of accounting records, donor histories and collections data."

As the nonprofit telling this story describes above, too often nonprofits are unprepared for technological losses. Let the words above be a cautionary tale: Now your nonprofit has no reason not to be prepared.

Being risk aware means acknowledging what *has happened* and imagining what *could happen*. When it comes to technology, there are tremendous upside risks to investing in the latest and greatest equipment. But with the boost that high-tech provides comes the need to maintain your nonprofit's peak performance and protect against sudden losses that can happen in a nanosecond.

Technology risks are diverse so your risk-imaginings need to be free-wheeling, realizing how expansively your nonprofit uses technology. Could any of these situations happen at your nonprofit?

- Employees using screensavers depicting sexual content/graphics;
- Harassment via email, voice messages or instant messaging;
- Employees or volunteers driving distractedly while talking on their cell phones;
- Employees or volunteers using the nonprofit's computers to view websites that contain pornographic material;
- Employees or volunteers using the nonprofit's computers for their personal for-profit business activities;
- Employees using copyrighted photos or graphics without permission;
- Data loss through a system crash, or a virus;
- Identity theft due to spyware on the nonprofit's system that captures financial and personal information,

including keystrokes that can unlock staff passwords;
- The invasion of your nonprofit's web site by Click Fraud (pop-up ads that just keep multiplying when you try 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;
- An employee's personal blog discusses work-related issues and identifies the nonprofit and colleagues by name.

Insurance for Cyber Losses

Cyber insurance protects against damages to computers and computer systems caused by human error or as a result of malicious attacks and crimes, including fraud, unauthorized access, theft of customer information and Web site sabotage. Loss of income from the interruption of your day-to-day activities, damage to data making it unrecoverable, and potential lawsuits are just some of the financial fallouts that may result from a data loss event.

While nothing can replace data that is permanently lost, or prevent a third party from bringing a lawsuit for losses they sustained when your computer system was breached, insurance products exist that can take some of the financial pain of the experience down a notch.

Most ordinary commercial general liability, and property and casualty liability policies won't cover data loss suffered by the nonprofit because electronic data is excluded from the definition of "tangible property." This means that nonprofits seeking insurance for cyber losses must find a special policy tailored to address computerized data losses.

- In some states (California and New York) "media" insurance policies are harder to come by. In most other states, separate data loss policies are more readily available, assuming that the nonprofit already has a back-up system in place to begin with. Luckily these special products are relatively inexpensive—a basic annual premium may be less than $1,000.
- To protect against lawsuits brought by third-parties, nonprofits can buy insurance that expressly covers the risk of causing a third party to suffer a data loss. That insurance may be called "internet liability," "cyber liability," or "network security" liability insurance.
- With the right insurance coverage for loss of computerized data your nonprofit may be able to:
    - Pay for staff time to re-enter data into a new database
    - Replace hardware that was damaged or destroyed
    - Pay a computer specialist to repair or resurrect a crashed or stolen file server
    - Pay for staff time to notify all customers or clients to let them know about a security breach
    - Pay for the cost of equipment needed to restore your nonprofit to the position it was in prior to the data loss event.
- With insurance for third-party liability suits your nonprofit may be able to:
    - Transfer much of the cost of defending the lawsuit to the insurance carrier
    - Pay the injured party the damages they claim resulted from a computer security breach or data loss affecting your nonprofit's computer system.
- For more information about data loss insurance policies, contact your broker or agent.

Enhancing the public's awareness of your nonprofit's activities and mission is one of the great byproducts of technology. It's easy to just "google" the name of a nonprofit and find all sorts of wonderful information with a few keystrokes. Those same keystrokes can undo many months and thousands of dollars of graphic design work, if your nonprofit has not taken steps to protect its web site. A malicious hacker can place unseemly content on your nonprofit's web site. Make sure that more than one person knows how to "shut down" your nonprofit's 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 that appears on the web site. Links from your nonprofit's web site to other sites can be misdirected or the links can become stale which impacts the impression viewers have when they visit your nonprofit's web site. Someone should be charged with the responsibility to conduct a regular review of all links from your nonprofit's web site. In order to claim the protections afforded by copyright laws, rigorous enforcement of any unauthorized use of your nonprofit's name

and logo is a must. 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.

Policies as well as vigilance are needed to protect the nonprofit's intellectual property, brand identity and good will in the community. Technology policies that are helpful in safeguarding a nonprofit's reputation include.

- **Code of Conduct** for employees
- **Photo and Video Image Policy and Release.** Photos and video images 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 or during work time, unless the blog is sanctioned by the nonprofit. (For more on blog policies see the Winter 2008 edition of Risk Management Essentials).
- **Responsible Use of Technology Policy.** The nonprofit's computers should not be used for illegal or inappropriate activity. When a policy spells out what is not permitted, volunteers and employees' use of computers and other technology is less likely to be inappropriate and employees/volunteers can be terminated for violations of the policy.

Policy Checklist

- 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
- Internet Access Agreement (for clients who are minors 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

Additional helpful checklists and sample policies are available from the Center's full length publication, *Full Speed Ahead: Managing Technology Risk in the Nonprofit World* which is currently available at a special promotion price of $10. Need help with a customized risk assessment for your nonprofit's technology risks or help developing appropriate policies to manage those risks? The Center can lend a hand. Send us an email! Protecting your investment in technology is prudent risk management.