Six Tips for Playing it Safe: At Work, At Home, On the Web

By Dennis M. Kirschbaum, ARM

Resource Type: Articles

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

We have all heard the saying, To err is human; to really foul things up requires a computer." The fact is, computers do not foul things up, people do. But computers allow us to foul them up faster, more efficiently and in more ways that we could have ever imagined. Computer technology has emerged from the ivory tower of the air-conditioned room and landed plop in the middle of our laps. It has also landed in our palms, our cars, our desks and even our kitchen appliances.

But technology [2] especially technology that is not well understood by those using it [2] can pose new challenges for organizations that have systems in place for handling paper documents and records. Sometimes it can be difficult to remember that information in the electronic world needs to be managed carefully.

First of all, make certain that your nonprofit has a policy in place that deals with technology related issues in the work place. Your policy should address the use of office computers and clarify that the computers provided by and used in the work place are for work purposes. Everything that is created and stored on those computers is subject to access by supervisors and perhaps co-workers.

The policy should also address:

- Proper use of email
- Restrictions on Internet access (if applicable)
- Use of personal electronic equipment in the office (e.g. laptop computers, personal organizers, etc)

Having a concise policy that describes your expectations can help avoid surprises later on. "I didn't know I wasn't supposed to play Internet Monopolyþ at work."

Imagine that your office has a strong metal door with a large dead bolt. You always keep it locked. Now imagine that the door has a dog flap. The door is not large enough for a person to go through. However, what you didn't realize is that somebody with the right tools can easily reach through the flap, and unlock the door.

"You have an obligation to protect the privacy of your clients. This is especially true if your organization serves vulnerable populations. If your client list includes youth, people with disabilities or people who are HIV positive, it could be devastating to you and your clients if the list finds its way into the wrong hands."

If you have a DSL, ISDN, or even a dial-up modem line into your computer system, it is like having a trap door

into your organization's computer system. Someone with the right tools can slip right in. Make sure that you have the right firewalls, password system, and monitors in place to assure that only the right people are "working from home."

You have an obligation to protect the privacy of your clients. This is especially true if your organization serves vulnerable populations. If your client list includes youth, people with disabilities or people who are HIV positive, it could be devastating to you and your clients if the list finds its way into the wrong hands. To protect your data, consult with a computer security expert. Also consider the following.

- Limit access to the client database and records to those who need it.
- Keep the database on a secure computer that is not on the local network.
- If you have a DSL line or other continuous connection to the Internet, make sure you have a secure firewall in place.

If you have minors who are using your organization's computers to access email or the Internet it is important to provide guidance on how to use the Internet safely. Monitor what kinds of web sites are being accessed and explain to kids that they should go to an adult if they ever feel uncomfortable with a contact they've made on the Internet or if someone asks them to meet them. A growing number of school districts provide training on safe web surfing and require students to sign "Acceptable Use Policies" or AUPs. Nonprofits that provide access to the Internet should consider developing similar policies.

In her new book, *Alphabet to Email: How Written English Evolved and Where It's Heading*, author Naomi S. Baron says that the nearly instant and often ephemeral nature of email leads people to think of it more as a phone conversation rather than as a form of written communica-tion. Email is often off the cuff, unedited and casual. People assume that email will just be deleted and disappear.

The fact is, email is not like a phone conversation, unless you routinely record your phone calls. Emails can remain on a server for a long time after the user thinks that they have been deleted. Messages may even remain in back-up files or on tape for years and could be retrieved or produced as part of a lawsuit. The lesson? Your email may have the staying power of words chiseled in granite.

If you think that the advent of the photocopier made it easy to steal others' work and intellectual property, the World Wide Web will take this unethical practice to new heights. Any information you post on your web site can be copied and pasted into other documents with ease. Even your logo can easily be copied. Domain name squatting has also become quite common. The practice involves registering a domain name that might be desired by another organization or one very similar. For example, your organization might register nonprofit.org and the squatter will register nonprofit.com and nonprofit.net. Then they will send you an offer to buy the names from them at a cost far beyond the $35 it cost them to register the names.

Hackers may also decide to disrupt your web site by taking it down or replacing your content. Why would they do that? Often they need no other reason than that they can. Even large organizations with huge resources like the *New York Times* have found themselves subject to such attacks. Many hours and dollars had to be invested to secure the site.

The point here is to raise awareness and to be sensitive to the risks of the information age, not to scare you into tossing all your computers out the window. As if you could! Technology is a part of our lives that is here to stay. Computers and the Internet are powerful tools. They make communication and access to information possible in ways that were unimaginable just a few short years ago. But along with the advances that technological progress brings, comes risks that need to be managed. With vigilance and attention to detail, you can avoid serious difficulties as you put the power of today's technologies to work in your nonprofit.

Dennis Kirschbaum is Manager of Information Technology at the Nonprofit Risk Management Center. He can be reached via e-mail or (202) 785-3891.