

Checklist for the Tech-Challenged CEO

A friend of mine recently became the CEO of a nonprofit organization. She's a person who appreciates technology but is not a technologist, so the question came up as to what she—and other CEOs in similar circumstances—might need to know about information technology. For example, would you know what to do if your IT person had to take an unplanned leave of absence? Or if the technology company to which you outsource your technology support went belly up?

Based on these questions and others, I developed (with the help of ASAE Technology Section listserver participants) a checklist of things that my friend could use to develop an understanding of the key elements of her organization's technology systems—and how she could hold things together during an emergency, while coming up with the necessary technology support to maintain the systems for the longer term. Learning the following details about your organization's technology will help you face an unexpected technology crisis with confidence and clarity.

■ **Accessing the system.** Establish procedures for accessing administrative passwords. Many organizations document this information on paper, floppy disk, or CD-ROM and then secure the data in a locked cabinet in case of emergency. Access is extremely limited. An updated log of key personnel with administrative rights to the applications should be reviewed periodically, specifically when staff changes occur. Make sure records include access information for servers and applications such as accounting, human resources, association management, online training, Web management, and backup systems.

■ **Maintaining backup procedures.** Ask yourself these questions: What are the association's backup procedures? What activity is backed up, how often, and how far back are archives kept? How often has the organization had to restore files, and what has been the success rate? Are tapes stored off site, and if so, how do you retrieve them if needed?

■ **Understanding minimum requirements.** Be aware of the routine data- or system-maintenance procedures that must run to avoid system or application problems. Include such details as log-file deletion, database reindexing, and so forth. Know also the reports or statistics that are run on a regular basis and the

staff people to whom they are delivered. Does the association provide any data to third parties from its database, and if so, how frequently, and under what circumstances?

■ **Gathering contact information.** Document the contract numbers and contact phone numbers for all maintenance programs. Verify that contact names and numbers are on file for noncontracted support vendors for other hardware or services. Also document all of the renewal dates and contacts for key subscriptions or services (such as Internet connectivity, domain name renewal, or maintenance programs that automatically renew).

■ **Securing the systems.** Answer the following questions: Do we have clearly documented rules regarding monitoring staff e-mails and other communication? How often has IT been asked to access staff information? Do we have protection against viruses and hackers? How are these maintained and updated? Do we have any remote access capabilities? If so, who has access and how confident are we that these methods are secure? Do we have a documented process for handling terminated employees or adding new employees? Do we have an inventory of all hardware and software, and if so, is it kept up to date?

■ **Establishing maintenance and purchasing responsibility.** Know who is responsible for handling the various technology-related elements of your operation. For example, in some associations, the office manager is in charge of setting up new users in the phone system, but the IT staff is responsible for troubleshooting the problems that users may have with the phones. Understand the purchasing-approval procedures for new hardware, software, and so forth, as well as the purchasing cycles (how often equipment is replaced, and what's coming due for replacement in the next several months or years).

A particularly problematic area can be ergonomics. For example, if a staff person needs a keyboard wrist rest, people may think that the IT department is supposed to buy it, when it may actually be treated as an office supply or human resources issue. While this generally would not fall in the category of emergency-related IT needs, it is still something to clarify when reviewing your entire IT strategy.

By reviewing these details early in your tenure at an organization, you can avoid the sense of panic and confusion in the event of a sudden loss of technology support.