Technology Mishaps: Planning for IT and Communications Disasters

By Christy Grano

Resource Type: Risk eNews

Topic: Business Continuity Planning, Data Privacy, Tech Risk, Cybersecurity

For most of us, the word “disaster” usually brings to mind a natural disaster like a hurricane or a tsunami, but in the risk management world technology disasters immediately come to mind. An unexpected loss of data or communication can bring an entire organization to a halt if power, internet, email, or cell service is compromised. Today, Information Technology professionals use the word “disaster” to refer to data loss—a disaster because the traumatic loss of records, websites, files, and other data is devastating to organizations. Data loss can be caused by internal mishaps like an employee losing a laptop, a sprinkler system going off in a server room, or a colleague accidentally wiping a financial record. Losses also come from outside an organization in the form of ransomware, phishing attacks, or other cybersecurity threats.

Unfortunately, many nonprofit leaders are unaware of where their data lives, much less what steps to take should it be lost. To combat technology risks thoughtful organizations develop *disaster recovery plans* to map out recovery strategies for various types of data loss, and *business continuity plans* that prepare the organization’s critical operations to continue running smoothly through a technology mishap.

Rather than anticipate every technology disaster that could occur, at NRMC we encourage nonprofit leaders to delve into tech risks by focusing on three areas of vulnerability: data, communication, and technology personnel. Here are some basic questions to ask yourself as you start to build your disaster recovery and business continuity plans with respect to technology:

1. **Data:** What kinds of data does your organization possess and use? It’s fairly certain that you have important data in the form of valuable emails, personnel information, financial records, and volunteer information. You could even have bank information in the form of copied checks, or passwords to bank accounts.More likely than not your organization’s data is growing. How much space is your critical data taking up, and how quickly is it expanding? Keep in mind that scans, photos, videos, and presentations can take up more space than other types of data.Every type of data lives somewhere, even data stored in “the cloud.” Where is the data in your possession physically stored? Are you aware of backup data and how it is stored? Are you backing up files to an external hard drive, for instance? Is this data kept current and secure?Be aware of how critical data can be restored if it is lost or compromised, and the *order of priority* if more than one type of data is lost. What data is the most critical to essential functions in your organization? In other words, when disaster occurs, which data should be restored first?
2. **Communication:** Many organizations plan for a breach in data, but not for a gap in communications.Upon what forms of communication does your organization depend most? Is there a

backup communication plan to get you through if power is lost, cell service is out, or an internet provider drops service?Your technology personnel should be aware of what communications are most critical to you in a crisis. Usually email and internet are the most important, but for some organizations internal networks or phone lines may come first. Do members of your team know what to do if go-to communications are unavailable?

3. **Personnel**: If your data and communications are managed by a single person, you're exposed to avoidable chaos or interruptions in service if that person is unexpectedly unavailable.Are your data and communications highly dependent on specific in-house or contract technology personnel?If that's the case, do you have a plan to cope in the absence of those key players?To what extent have others been cross-trained to step up and pitch in to manage and trouble-shoot systems and IT resources when the principal players are on injured reserve?Better yet, have these steps and process been documented in a desk manual, procedures document, or simple *how-to* guide that has been customized for your IT environment.

If your answer is 'no' or worse, "I don't know," resolve to get up to speed with the answers *before* the data is lost, the phone lines are down, or the webmaster gets the measles! You don't want to be taking care of your technology *on the fly* in mission critical situations.

Planning for technology mishaps

A bit of good news is that since technology concerns and risks are virtually universal—regardless of organization type or size—there are countless resources, advisors, and tools to help organizations of any size anticipate and prepare for technology mishaps. With so much critical information being sent back and forth on the internet today, technology providers are motivated to provide secure data solutions. With the help of a knowledgeable IT professional, affordable plans can usually be created to prepare for most types of technology loss.

Reinforce and test your plans!

After identifying assets and exposures related to data, communication and personnel, it's time to put a plan in place that will reduce the time it takes to get back up and running with your regular IT assets and resources. Don't forget to test and reinforce your recovery and back up plans. Organizations that conduct emergency drills and tests are much more likely to find calm in the storm of a true crisis. Reinforcing your policies and practices can be as simple as reminding employees where an emergency handbook can be found, including your plan as part of new employee orientation sessions, or conducting periodic data recovery exercises. A robust, tested plan will be well worth it when a real technology disaster arrives.

Resources

For additional information on risks related to technology use, see these additional NRMC resources:

- Pass the Remote! The Trials, Tribulations and Triumphs of Telecommuting Teams
- Social Engineering: Why People with Passwords are the Biggest Threat to Your Mission
- Cyberbullying & Cyber Threats to Young People
- Good Measures: Reassessing Your Social Media Response