Planning for the Quiet Disasters: Technology Mishaps

Ask yourself these questions about your vulnerable areas.

By Christy Grano

When you hear the word "disaster," you probably think of natural disasters such as hurricanes. 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, e-mail, or cell service is compromised.

Information-technology professionals use the word "disaster" to refer to data loss because the loss of records, websites, files, and other data is so devastating to an organization. This kind of disaster 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 in the form of ransomware, phishing attacks, or other cybersecurity threats.

Unfortunately, many nonprofit leaders are unaware of where their technology and data live, much less what steps to take if they are lost. To combat technology risks, thoughtful organizations develop two things:

- **disaster recovery plans** to map out recovery strategies for various types of data loss
- **business continuity plans** to assure that critical operations continue through a technology mishap.

Ask These Questions about Three Key Areas

Rather than anticipate every technology disaster that could occur, delve into tech risks by focusing on three areas of vulnerability:

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 e-mails, personnel files, financial records, and volunteer information. You could even have bank information in the form of copied checks or passwords to bank accounts.

How much space is your information taking up, and how quickly is it growing? Keep in mind that scans, photos, videos, and presentations can take up more space than other types of data.

Where is your information physically stored? Every type of data lives somewhere, even data stored in "the cloud."

> "Loss of data can bring an organization to a halt."

Are you aware of backup information and how it's stored?

Do you know how to restore information if it is lost or compromised?

What is the order of priority if more than one type of data is lost? What information is most critical to essential functions in your organization? When disaster occurs, which data should be restored first?

2. Communication:

What forms of communication does your organization depend on most? Many organizations plan for a breach in data but not for a gap in communications. E-mail, text, and cell phones are likely the lifeblood of your organization, so it's essential that you know what to do if these forms of communication are lost.

Are there backup communications to get you through bumps in the road if power is lost, cell service is out, or an internet provider drops service?

Do you know what communications are most critical in a crisis so you know where to focus first? Usually e-mail 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:

Are your data and communications highly dependent on specific in-house or contract personnel? If that's the case, do you have a plan to cope in the absence of those key players? 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.

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?

Have you documented these steps and processes in a desk manual, procedures document, or simple "how to" guide customized for your IT environment?

If your answer to any of these questions is "I don't know," resolve to get up to speed with the answers *before* the information is lost, the phone lines are down, or the webmaster gets the measles!

Plan for Technology Problems

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 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 be created to prepare for most types of technology loss.

Reinforce & Test Your Plans

After identifying assets and exposures related to data, communication, and personnel, it's time to put a plan in place to reduce the time it takes to get back up and running with your regular IT resources. Don't forget to test and reinforce your recovery and backup 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 doing the following:

- **reminding employees** where an emergency handbook can be found
- **including your plan** as part of new-employee orientation sessions
- **conducting data-recovery exercises** on a regular basis.

A robust, tested plan will be well worth it when a real technology disaster arrives.

Christy Grano (christy@nonprofitrisk.org) is senior consultant at the Nonprofit Risk Management Center. The Center teaches leadership teams how to take thoughtful risks and make their nonprofit missions more resilient.

Lessen Your Vulnerability

Learn more ways to reduce tech risks at NonprofitWorld.org:

Don't Get Caught by Phishing Schemes (Vol. 35, No. 2)

Nine Surefire Steps to Lock Down Your Cybersecurity (Vol. 36, No. 3)

Wire Transfer Fraud: It Could Happen to You (Vol. 35, No. 3)

Keep Your Online Identity Safe (Vol. 35, No. 4)

The Purposeful Techie: Nonprofit IT with Intention (Vol. 30, No. 5)

What to Do When an Employee Becomes a Cybercriminal (Vol. 39, No. 4)

Don't Go It Alone in a Crisis (Vol. 37, No. 2)

Mitigate Cyber Risks with the Right Security Controls (Vol. 36, No. 1)