Think about all of your nonprofit’s assets, from the computers and servers around your office to the data you store on them. What would you do if something bad happened to them?

Disaster can take many forms, from the natural—floods, tornados, earthquakes, pandemics—to those caused by humans—fires, theft, cyberattack, power outage. It also includes the unintentional—such as a well-meaning staff member accidentally deleting your entire database—and more predictable disasters, like a malfunctioning server or computer crash taking your network offline.

It doesn’t have to be a big, full-scale disaster, either. It might be something as simple as your phone systems going down unexpectedly. Would your staff still be able to carry out essential work?

IT professionals say there are two types of organizations: those that have experienced some type of disaster, and those that have not... yet. Maybe your nonprofit is one of the lucky ones. But as they say, “luck” is not a plan. There’s a good chance that some kind of disaster—natural, self-inflicted, or malicious—will occur during the life of your organization. To protect yourself, your staff, and your constituents, you need to plan ahead to be ready for it.

The primary goal of any organization in a disaster should of course be safety—preventing the loss of life and protecting staff. This article is focused on technology disaster recovery planning. Disaster recovery means planning for the worst by increasing redundancy, working to eliminate single points of failure, and ensuring you have working backups.
The goal of any good disaster recovery plan is three-fold. First, ensuring that all data is recoverable so that no information is lost in the long term; second, minimizing any IT downtime; and third, planning for continuity so that staff can keep operations running until everything is fully recovered and operational.

Your plan should be a written document. At a high level, it should identify potential threats, outline steps to minimize risks, and establish procedures to follow after a disaster. It should be a living document that is reviewed and improved several times a year.

**Personnel**

In the event of a disaster, who is in charge of your response? The time to designate personnel is *before* you need them to act. Consider who is best able to evaluate the situation, determine the steps necessary to get things back to normal, and communicate with the rest of the organization or relevant personnel or authorities, and assemble a team. This team’s responsibilities might include the following:

- Evaluating the magnitude of the disaster and what systems and resources have been affected.
- Setting the disaster recovery plan into motion.
- Communicating with other relevant personnel.
- Determining and assigning first steps.
- Setting expectations and goals.

Identify team members and make sure their roles are clear. Do you have personal contact information for every staff member? If you don’t know how to reach them, you’re already at a disadvantage.

How will an outage affect staff members’ ability to communicate with one another and with the outside world? Do volunteers or other people who are not staff members use your organization’s technology infrastructure, including phones or email addresses? In the event of a natural disaster, what is the process for contacting and accounting for each staff member to verify that they are safe and able to help with the recovery process?

**Redundancy of Responsibility**

In the event of a disaster, you may not be able to reach the person who would normally be responsible for IT. For example, Tech Impact’s Backup and Recovery Engineer George Staton recalled the time Super Storm Sandy devastated the East Coast and left him without power or cell phone service while he was working in infrastructure management at a previous job. The storm also took down all of his company’s networks.

Fortunately, Staton and his team had prepared in advance of the coming storm. By delegating his authority to a staff member on the west coast, outside the storm’s reach, he had made sure that someone had the full authority to make the decisions necessary to get the company’s networks back up and running—even while he remained out of contact.

A good disaster recovery plan will identify staff roles in a disaster and include secondary people to step in if the primaries are not available.

**Systems and Resources**

Your plan should also identify the functions or services most essential to your organization or constituents in priority order. List and prioritize based on importance in helping carry out those essential functions or services, and detail how you will go about replacing them if they are damaged or destroyed. Documenting this in your plan creates a single, reliable list of information—but that means you need to revisit this list multiple times each year to make sure you are keeping pace with new equipment or systems.

What equipment do you have in your office? This should be exhaustive, and include hardware, networks, and systems—not just computer networks but telephone systems, but data systems, financial and accounting systems, etc...
What equipment might staff members have at home or offsite that could be repurposed or called into action until the main systems are back online?

Do you have maintenance and update logs, vendor contact information, user login and password information? Where will you purchase or acquire new hardware? Is data held remotely in the cloud, or in the office? If data is in multiple locations, specify what is where. Where are your data backups held? Whose role is it to restore the backups?

You should not only have a plan for restoring backed up data, but you should be comfortable with the process and confident in your ability to implement it quickly.

Are you confident in the steps needed to restore a backup? If not, practice until you are.

Backup and Recovery
A backup strategy to prevent the cost and effort of recovering from data loss is made up of two components: the media, and the method. The method determines what information you’ll backup and when. The media is the form backups will take.

Local backups—like external hard drives, network drives or removable media—guard against physical failure of a hard drive or server, but not severe events like fire, flood, theft or virus. Remote backups, which transfer data to shared storage centers via an Internet connection, excel in individual file- or folder-retrieval. The best backup strategy includes a combination of the two.

In most cases, data restoration from a local backup is going to be significantly faster than from remote, which can take from a few hours to a few days. Most remote backup solutions also don’t let you restore a system from a bare computer, including the operating system and software applications.

Local backups are primarily physical solutions, like removable media, used to backup an entire server. Remote backups are software solutions installed on each computer or server.

When signing a contract with any cloud provider, whether for remote storage and backup solutions or server-based software platforms, make sure your vendor has contingency plans for disaster recovery. Just because you’re outsourcing your oversight

You should not only have a plan for restoring backed up data, but you should be comfortable with the process and confident in your ability to implement it quickly.

What Should You Back Up?
The simple answer is, “everything.” Or at least, everything that’s critical, valuable, irreplaceable or important to your organization. Consider each of your organization’s processes separately and account for each by identifying and backing up its data. And remember, backing up file servers won’t do any good if individual staff members are storing their valuable data on local hard drives. Make sure networked computers all have access to file storage, and that everyone on staff is using it.

Don’t forget about paper data. Backing up online data is relatively easy, thanks to the cloud—but not all data lives in bits and bytes. Your organization may have paper records that need to be backed up, including, for example, hardware warranties and receipts or archival files. Ideally, such files should be digitized and backed up like your other online data, but at a minimum, paper records should be stored in a cool, dry place that is less susceptible to a natural disaster or fire.
Planning for Your Plan
Creating a plan is important, but it isn't enough. Staff members will be more confident in their organization’s response—and less likely to muddy the waters by acting independently of the plan—if they’re familiar with the plan in advance of when it is needed.

Share the plan with the organization and train relevant staff members to help them stay safe in the event of an emergency.

You can’t prepare for all disasters, and you can’t stop them from happening. But with a little bit of forethought, you can be ready for them when they do.

Join us Thursday, May 12, from 11 AM-12 PM Eastern, for a FREE webinar on disaster recovery planning. Tech Impact Expert Trainer Joel Barker will walk you through the different types of potential disasters and guide you in developing a plan to get your organization back up and running as quickly and safely as possible.

Sign up for free at https://techimpact.tovuti.io/events-cal/technology-strategy-governance/disaster-recovery

Minimizing Risk
What are the most likely disasters in your area? For example, West Coast offices might be most concerned about earthquakes, while Midwestern offices could be more likely to experience floods or tornados. List your location’s top disaster threats. Does seeing this list change any of your plans?

Review your insurance policies. Do they cover lost time, location rental, recovery services, and equipment and device replacement? Knowing what money you will have to support your recovery will help you determine what to recover and how quickly you can get it running again.

Where will you store your plans? It won’t do you any good to have a plan if it burns up in a fire. Keep everything on a flash drive (maybe more than one) and in a secure location away from your office.

doesn’t mean that you can stop paying attention, Staton said.

“You’re still accountable for that data—read your contract,” he said. “There should be a disaster recovery component, and if not, ask for it.”

The language should “more or less align” with the information in this article, he said, following disaster recovery planning best practices.

“Generally speaking, the big vendors’ disaster planning is probably better than anything you can put together on your own,” he said. “Just don’t take it for granted.”

About Tech Impact
Tech Impact is a nonprofit that leverages technology to advance social impact. Our proven workforce training programs and intermediary services prepare our graduates to launch or advance their careers in technology. Through a full spectrum of technological support, we give nonprofits the technology, education, and solutions they need to deliver greater impact and help their communities thrive. Learn more at techimpact.org, or browse the hundreds of free publications and educational resources in our Technology Learning Center at techimpact.org/technology-learning-center.

About the Authors
Chris Bernard is Tech Impact’s Managing Editor and oversees the organization’s research and editorial efforts.

George Staton is Tech Impact’s Backup and Recovery Engineer and works with a wide range of nonprofits.