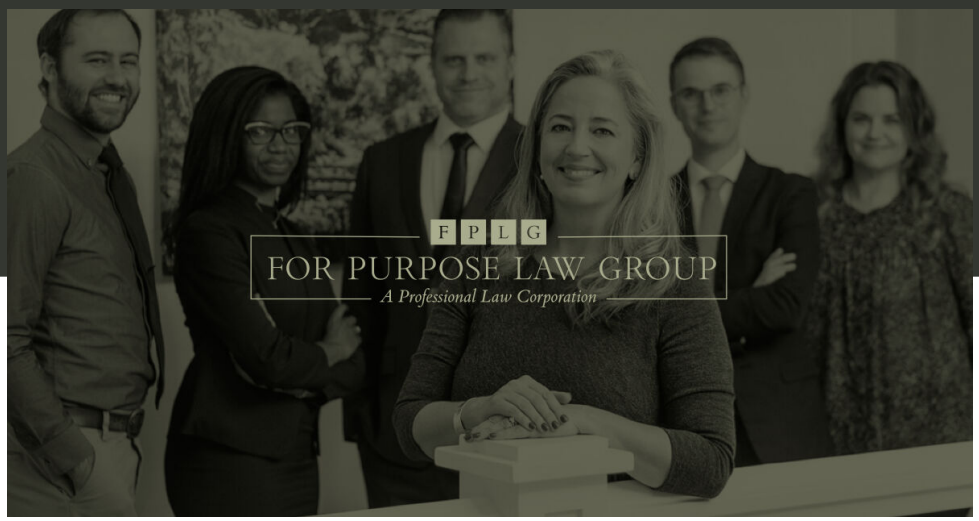
FPLG
FOR PURPOSE LAW GROUP
A Professional Law Corporation

NONPROFIT

Nonprofits and Disaster Preparedness

09.21.18 | Linda J. Rosenthal, JD



Each year at the start of hurricane season in the U.S., we're reminded of the enormous potential for damage and disruption. Of course, natural disasters can (and do) strike anywhere – often without any warning.

Disaster planning and preparedness are not the same in 2018 as they were even a decade or so ago. In addition to more advanced weather-prediction tools to give us more advance warning for certain types of events like hurricanes or tornadoes, there are now important technological advances that let us store vast amounts of data away from our physical location (that is, the site of the disaster) and operate as a team at a distance.

Disaster Planning is Critical

A nonprofit organization not only has to take steps to minimize harm to its personnel and property and to continue operating through the emergency and beyond, but also, in some cases, to provide emergency services to its community.

What should nonprofits do to "ensure they can withstand any storm?" Phil Goldstein of BizTech says "[t]hey should develop and practice a disaster recovery plan, back up their data, invest in backup power supplies and telework solutions, and prepare their infrastructure for any power outages."

Create a Plan

The first step in adequate disaster preparedness is to create a plan well in advance. It should include a determination of how a disaster might affect the operations of the nonprofit. "Nonprofit IT leaders should work with management to assess the organization's needs, requirements, budget, and IT environment." For smaller organizations, there are outside firms which can help with these assessments.

This advance plan "should encompass people, processes and technology."

Once the plan is created, it should be tested by "simulating a disaster."

Back Up Data

A critical part of disaster planning is making an inventory of the organization's data and where it is located, and then backing up this important information. This involves replicating the files: copying them from the primary site to a secondary location. "For added redundancy, nonprofits should partner with a cloud service provider to back up data to the cloud" for easy restoration after the emergency.

Part of this process includes periodically checking the backup and adding newly created data.

Back Up Power

An often overlooked-element of disaster readiness is a having a method to generate power if the supply is cut off. According to Tech Impact, "[t]o protect your machines from losing power (blackout) or not getting enough power (brownout), invest in an uninterrupted power supply (UPS) and make sure it is configured properly."

The benefit of a UPS is that it can keep your organization's IT equipment on for a while, at least, when electrical power is lost during the disaster. If it's set up correctly, there is a signal sent to the equipment to "gracefully shut down after a certain period of time." Without it, the equipment will shut off abruptly.

Set Up Telecommunications

The organization should "establish telework capabilities with mobile devices, cloud services or virtual desktop environments." In addition, have "soft phones or call-forwarding services" so that calls to landlines will be redirected.

Conclusion

Particularly after the extreme weather events last year all around the globe, experts have focused on, and written about, this technology aspect of emergency preparedness. "By plotting out technology and policy strategies, businesses [and nonprofits, of course] establish continuity plans to prepare for any disaster."

Of course, in addition to natural disasters, a nonprofit's IT operation can be disrupted by other sudden causes including "system failures, security breaches and human errors." So creating and implementing a technology emergency plan is critical to making it through a variety of crises.