Is your business prepared for an emergency? Is your data?

Lesley Fair
Sep 4, 2018

When an emergency strikes, your business's most vulnerable asset may not be in the stockroom or warehouse. It could be the data that has been central to your success. September is National Preparedness Month. The FTC has six steps you can take to help protect your company's information from the unpredictable.

Conduct an information inventory.

While the skies are sunny, take an inventory of the data critical to your business – customer lists, invoices, personnel files, tax records, etc. For a home-based business, it may be a matter of one computer. For other companies, consider what's on your network, smartphones, office desktops and laptops, and employees' home computers. Don't forget paper records in cabinets and file rooms. Knowing what you have and where you have it is the first step toward creating a preparedness plan.

Streamline what you retain.

Some companies' record keeping is the informational equivalent of that last warehouse scene in *Raiders of the Lost Ark*. Of course, there is material you must maintain. But to prepare for an emergency, it's easier – and less expensive – to protect a smaller amount of data. (A sensible plan to securely dispose of electronic files and paperwork you no longer need has the additional benefit of helping your company start with security.)

Back up essential information.

We've all heard data disaster stories: file cabinets floating down a flooded Main Street or confidential records blown miles away by a tornado. And it doesn't have to be weather-related. A broken pipe or a fire in the building next door can put your information at risk, too. The best preventive measure is a sound plan for backing up your business records – both digitized data and paper files. Depending on the size and nature of your company, you have lots of options: flash drives, external hard drives, online back-up, and cloud storage, to name just a few.

Take special steps to secure back-up files.

A meticulously maintained back-up won't be of much good if it's kept in an office damaged by disaster and it could pose the risk of a data breach if off-site storage isn't secure. So give careful thought about both how and where to maintain your back-up files. Keep your back-up up to date and consider encryption for sensitive information.

Think through how emergencies elsewhere could impact essential services.

When it comes to service providers, it really is a small world after all. That's why a storm in Sarasota or a blizzard in Butte can impact companies across the country and around the world. Do you have contingency plans in your contracts if an outage elsewhere impacts your information operations?

Follow time-tested advice at home – and at your home-away-from-home.

The FTC just published a new article for consumers about financial readiness in times of emergency. Share it with your employees to help create a resilient workplace. (Many of the tips apply to businesses, too.) In addition, the Small Business Administration has advice for companies about preparing for all kinds of emergencies and the Department of Homeland Security's "Ready" initiative has toolkits for business in English and Spanish.