

Disaster Preparedness

Advice You Can Depend On To Weather Any Storm



Office DEPOT®

Disaster Planning and Recovery...



is about developing an effective response to a crisis — and preventing that crisis from becoming a full-fledged disaster.

At its core, preparing for a disaster is about business survival. Having a sound contingency plan can enable your small business to successfully “weather” any storm – be that a hurricane, tornado or flood, as well as a technology disaster, such as a computer virus or a power outage that can happen at any time and without warning.

On average:

- 20% of all small to medium businesses suffer a disaster every 5 years.
- 43% of businesses damaged in a disaster close for good. That figure rises to nearly 60 percent after a year, according to the Association of Small Business Development Centers.

According to experts, there are two primary goals to disaster planning:

- Prevent** disruptive events that can be anticipated; and
- Reduce** the impact of disruptive events that are unavoidable.

Not having a contingency plan or backup systems in place can mean shuttering your business, so it is critical for businesses to take disaster planning seriously.

Having weathered four major hurricanes last year alone at its corporate headquarters in South Florida and 60 of its Gulf State stores, Office Depot has real world experience and practical solutions to help businesses deal with disruption. This brochure contains valuable advice from Office Depot’s Global Business Continuity Team, led by Director Tom Serio, and Jon Toigo, an IT veteran and author of numerous books, including *Disaster Recovery Planning: Preparing for the Unthinkable, 3rd Edition*.

“It is time to apply pragmatism, common sense, and energy to disaster preparation,” says Toigo, an experienced disaster recovery planner who has assisted small, medium and large sized firms in developing appropriate disaster plans for their business.

Serio emphasizes, “Plan, plan, plan.

Have a continuum as a disaster unfolds. It doesn’t have to be a million dollar solution, just a common sense one that protects you, your employees and your business.”

The overarching principle in disaster planning and recovery is to protect your most valuable and irreplaceable assets: your people and your data.

Protect Your People



Employees are a company's most important resource. Remember, in times of disaster, it's not business as usual. Focus must be on helping employees navigate personal issues, from damaged homes to personal injury. Office Depot's Serio says this type of employee support will come back to the company in the form of loyalty. "Time and again, I've seen employees choose to prioritize work over reassembling disrupted lives because it's the only bit of normalcy they have. As an employer, you want to strive to make this difficult period as easy as possible."

Serio notes that the most critical aspect of emergency planning is getting employees to think ahead. To protect your employees through a disaster, he recommends you take these four key steps.

1. Build Solid Contact Lists

Keep contact information for the following updated and easily accessible:

- Employees.** Maintain complete information for communicating with extended family members, too. Include home/cell phone numbers and email addresses for next of kin, and spouses/relatives; don't forget to make use of text-messaging capabilities and other communications devices as they may be the only way to stay in touch.

- Emergency phone numbers.** Include local fire and police departments, hospitals and ambulance services, building security, utility companies, as well as government disaster-relief agencies.
- Key vendors and suppliers.** Have ready a list of vendors and suppliers that can be relied upon to respond quickly.

2. Establish Emergency Communications Procedures

Establish a clear process for communications and plan how you will contact one another in different scenarios. Meet with your employees periodically to review emergency plans.



Protect Your People



3. Organize Supplies

Make sure the company and its outposts have access to cash, generators, batteries and supplies, such as first aid kits, ice, water, personal care supplies and food (e.g., nuts, dried fruits, and canned foods), and the ability to charge cell phones and communication devices.

4. Provide Employee Assistance

Train a staff member in CPR and first aid. Also, prepare Family Disaster Kits for employees that include food and resources, including:

- Flashlights
- Batteries in various sizes
- First aid kit
- A battery powered radio
- Plastic containers to seal critical information
- Disposable camera
- Hygiene supplies
- Post-event cleaning supplies
- Travel maps



Protect Your Data



Businesses rely on technology now more than ever. “We can no longer afford to wait even 48 to 72 hours to recover mission-critical data like we could five years ago,” according to Toigo. “**Today, if you lose your data, you can lose your business.**”

“A company denied access to its business data for longer than 48 hours is very likely to never recover fully from an outage. Those that take longer than four days to restore their data to an accessible form tend to be out of business within a year,” says Toigo.

According to a recent survey conducted for *Disaster Resource Guide*, network interruption is the second leading cause of business stoppage.

Toigo’s top recommendation for protecting data:
Make a back-up and move the media to an off-site storage facility.

These helpful solutions will guide your efforts.

Know How To Store Data

The right data storage solution is dictated by the importance and quantity of data you need to protect, the timeframe for restoration, and of course, your budget. Here are two:

- Copy data to removable media, including DVD-R or CD-R discs, tapes or to removable disk drives that connect to systems via their USB ports.
- For larger volumes of data that require quick restoration, look for specialized software for continuous data copy, or use an e-vaulting company to which you can send your data electronically for secure back-up and storage.

Back-Up Data On A Regular Schedule

To protect your business from faltering after a disaster, you will want to:

- Back-up your key data at least every week.** If you don’t have a tape back-up system, make copies of your most important data on CDs, portable disk drives that quickly connect to your computer’s USB port, or even to a laptop.



Protect Your Data

5

- Take a copy of your software used to make back-ups to a secure off-site location.** You will need it to restore your data from tape. Follow these guidelines:

- Don't leave your back-ups sitting next to your systems.
- Move back-up media to a secured, alternate or off-site location.
- Replace the media with the next week's back-up.
- Make sure to mark the media with content and dates.

- Store copies of key forms and hard copy documents you use in day-to-day operations at a safe location.**

Have them available to help you keep your business functioning.

- A simple consultation with your operations people will guide you to critical application software and documents you should protect.
- Scan key documents (e.g., insurance) into the computer for electronic storage.
- Include photos of major building and manufacturing sites, protected in watertight storage containers and stored in a fireproof safe, in case you need to present them to your insurers.

- Periodically review the data being stored on any back-up systems.** You will want to ensure that the right data is being copied and that it can be restored.



OFFICE DEPOT'S DISASTER Preparedness Checklist

6

Prevent What Is Preventable

Protection and prevention are core values of any disaster recovery strategy. Following is a checklist of products that will help you to avoid or reduce the impact of preventable disasters.

Protection



Laptop with durable hardware enhancements (e.g., shock absorber)



Flash memory drive



External hard drive



Writable CDs and DVDs, CD-Burners



Zip® drive



Mobile Folding File Cart



Surge protector and battery backup



Fireproof safe



Security box with fire-retardant insulation



Camera/film or digital camera



Scanner

Prevention



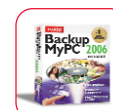
Smoke alarm



Fire extinguisher



Security management software (i.e. antivirus, antispam)



Systems management software



Network management software (monitor hackers, denial of service attacks, etc)

OFFICE DEPOT'S DISASTER Recovery Checklist

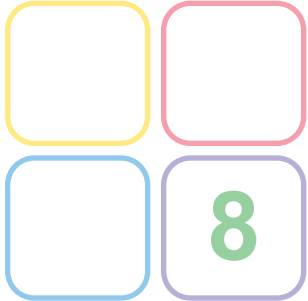


Helpful solutions to weather any storm

- Battery-powered weather radio and extra batteries
- First aid kit
- Flashlights
- Waterproof plastic bags
- Sandbags, shutters
- Pens/Pencils/Paper
- Water/Food supplies
- Generator
- Garbage bags, filter mask, mops, pails, etc. for sanitation
- Tool kit
- Contact sheets of employees, vendors and local emergency agencies



Invest in Preparation



The cost of your disaster recovery planning measures will depend on the nature and size of your business, the potential hazards, and the types of preventive and protective strategies required.

In the final analysis, those who prepare for the possibility of a disaster are much more likely to recover from one than those who don't. The bottom line is you can't afford not to be prepared.

The bottom line is you can't afford not to be prepared.

Building Your Disaster Preparedness & Recovery Plan: How To Get Started

9

A disaster recovery plan should be flexible — built on the basis of a catastrophic disaster that requires you to evacuate has occurred, but able to be scaled back easily to respond to lesser events.

Get A Commitment From Upper Management For Resources. The key is to build a business case that outlines value beyond simple risk reduction. Disaster recovery planning is not “just more insurance.” Consider how the analysis can improve the cost-efficiency of business operations and technology investments, for example.

Collect Data and Analyze Risk. To give a structure to your recovery plans and help prioritize recovery goals, determine:

- Your mission-critical business processes;
- The technology that supports these processes;
- The data these processes produce and use; and
- How that data is presently being stored.

Determine Objectives, then Strategies. Identify your goals for recovery, including how quickly your key business processes need to be back up and running. Then, create the appropriate recovery strategies.

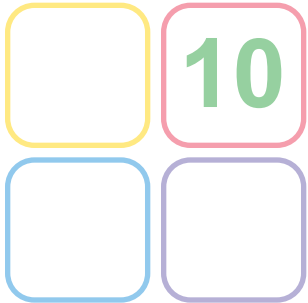
Most companies need specific plans for the recovery of 1) the applications and their data that support key business processes; 2) voice and data networks; and user work areas (e.g., at home).

To help minimize the impact of a disaster and recover critical functions:

- Develop a plan to recover the communications and storage networks that provide access to applications and their data.
- Devise a strategy to enable users to set up shop and perform useful work following a disaster. Ensure users have the resources to perform their jobs, whether at a new work location or from their homes.



Building Your Disaster Preparedness & Recovery Plan: How To Get Started



Staff the Plan and Train Your Personnel. The real value of disaster recovery planning is its role as a rehearsal. By training and testing key personnel about their role in an emergency, you are preparing them to think and behave rationally in the face of a great irrationality: a disaster. Some pointers:

- Build teams of two or more people (a primary person and a back-up) to handle key functions in an emergency. Make sure they are both fully empowered to make decisions for their areas.
- Beyond technical tasks, such as system or network restoration, assign responsibilities to specific teams for:
 - Managing employee communications;
 - Handling transactions with vendors and suppliers;
 - Overseeing salvage and insurance assessments; and
 - Managing media communications.
- Management will need to participate in ongoing training and rehearsal.

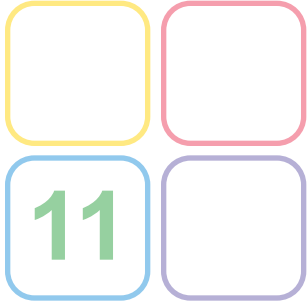
Test the Plan. Testing is the only way to spot gaps and make necessary changes - without testing, planning has no value. Establish an ongoing schedule of routine tests, including spontaneous ones.

Centralize Knowledge. Centralize all information in a database or an intranet site. It is much easier to keep the details of the plan up-to-date, and to report on changes, if all the information is centralized and readily accessible. And, always retain a copy off-site that can be easily obtained. Many companies keep their plans online but have back-up hardcopies at other locations.

As a practical matter, make sure you know and document the details of your flood insurance and other hazard insurance policies, specifically which items and contents are covered, and under what conditions. You may need to buy separate insurance for these threats. But, there is good news — many carriers will reduce your insurance premiums for business continuity insurance if they know you've taken the above precautions.



Additional Resources



- The U.S. Department of Homeland Security's Ready.gov (www.ready.gov) is a common sense framework designed to launch a process of learning about citizen preparedness.
- The Small Business Administration (www.sba.gov) provides disaster relief loans to qualifying businesses after disasters.
- American Red Cross (www.redcross.org) offers disaster planning information and emergency training.
- Disaster Recovery Planning.org (www.drplanning.org) and the Data Management Institute (www.datainstitute.org) are two comprehensive online resources for disaster recovery and data protection planning.